Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
”КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО”

Захаріудакіс Лефтеріс
(Греція)

УДК 004.052.42

МЕТОДИ І ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ РОЗПОДІЛЕНИХ СИСТЕМ

Спеціальність 05.13.05 – Комп’ютерні системи та компоненти

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ - 2017

Дисертацією є рукопис.

Робота виконана на кафедрі обчислювальної техніки Національного технічного університету України ”Київський політехнічний інститут імені Ігоря Сікорського”.

Науковий керівник – доктор технічних наук, доцент
Стіренко Сергій Григорович,
КПІ ім. Ігоря Сікорського, завідуючий кафедрою обчислювальної техніки

Офіційні опоненти: доктор технічних наук, професор
Додонов Олександр Георгієвич,
Інститут проблем реєстрації інформації НАН України, заступник директора

кандидат технічних наук,
старший науковий співробітник
Чемерис Олександр Анатолійович,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, провідний науковий співробітник

Захист відбудеться 29 січня 2018 р. о 16-30 годині на засіданні спеціалізованої ради Д 26.002.02 у КПІ ім. Ігоря Сікорського (м. Київ, проспект Перемоги 37, корп.18, ауд.516)

З дисертацією можна ознайомитися в бібліотеці Національного технічного університету України ”Київський політехнічний інститут імені Ігоря Сікорського”.

Відзиви на автореферат у двох примірниках, завірені печаткою установи, просимо надсилати на адресу: 03056, м. Київ, проспект Перемоги 37, вченому секретарю КПІ ім. Ігоря Сікорського.

Автореферат розісланий ”__” грудня 2017 р.

Вчений секретар
спеціалізованої вченої ради Д 26.002.02 Орлова М.М.
кандидат технічних наук, доцент

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. З появою технологій комп'ютерних мереж прогрес в більшості областей людської діяльності значною мірою визначається інтеграцією інформаційних ресурсів. Можливість доступу до якісно більш широких об'ємів інформації дозволяє значно підвищити якість прийняття рішень та проектів, прискорити та здешевити їх розробку.

Необхідною умовою інформаційної інтеграції є застосування ефективних механізмів контролю доступу до даних. Ключову роль серед них займають засоби ідентифікації та автентифікації віддалених абонентів.

Поява та динамічний розвиток хмарних технологій знаменує собою якісно новий етап інформаційної інтеграції. Фактично, в рамках цих технологій, категорія інтеграції збагачується новим змістом: крім інформаційної складової, забезпечується інтеграція обчислювальних та програмних ресурсів на комерційній основі. З іншого боку, якісна зміна інформаційної інтеграції, ініційована появою хмарних технологій, вимагає адекватного розвитку механізмів контролю доступу користувачів до віддалених інформаційних та обчислювальних ресурсів і, в першу голову, засобів ідентифікації та автентифікації абонентів інтегрованих систем.

Широке розповсюдження хмарних технологій надає користувачам значні за обсягом обчислювальні ресурси, які можуть бути використані потенційними зловмисниками для порушення існуючих механізмів контролю доступу до інформації. Це об'єктивно вимагає прийняття заходів для підвищення надійності механізмів ідентифікації віддалених користувачів. Разом з тим, поява хмарних технологій має наслідком значне зростання кількості користувачів, для якісного обслуговування яких потрібно радикально прискорити процедури контролю їх доступу до інформаційних та обчислювальних ресурсів.

Таким чином, наукова задача підвищення ефективності засобів ідентифікації та автентифікації віддалених користувачів є актуальною та практично важливою з огляду особливостей сучасного етапу розвитку інформаційних та комп'ютерних технологій.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось на кафедрі обчислювальної техніки КПІ імені Ігоря Сікорського в рамках держбюджетної теми "Розробка теоретичних основ побудови високопродуктивних комп'ютерних систем з динамічним розпар алелюванням обчислювальних процесів" (номер держреєстрації 0111U002729) згідно з науковим напрямком "Розробка високопродуктивних багато кластерних обчислювальних систем".

Мета і завдання дослідження. Метою роботи є підвищення ефективності ідентифікації віддалених користувачів розподілених систем за рахунок прискорення криптографічно строгої, основаної на концепції "нульових знань", ідентифікації шляхом розробки методів її комп'ютерної реалізації з

використанням незворотних перетворень булевої алгебри та алгебри скінчених полів Галуа.

Основні задачі дослідження у відповідності до поставленої мети полягають у наступному :

1. Аналіз загроз несанкціонованого доступу до ресурсів в розподілених системах. Обґрунтування, на основі результатів аналізу, вимог до систем ідентифікації користувачів та критеріїв їх ефективності. Огляд сучасного стану засобів ідентифікації віддалених користувачів розподілених систем та тенденцій їх розвитку.

2. Виявлення можливостей підвищення ефективності ідентифікації віддалених користувачів за рахунок зниження ризику несанкціонованого доступу до ресурсів розподілених систем та підвищення продуктивності засобів ідентифікації.

3. Теоретичні дослідження можливостей реалізації строгої ідентифікації користувачів у відповідності з теоретичною моделлю “нульових знань” з використанням незворотних перетворень в альтернативних математичних алгебрах, зокрема булевої алгебри та алгебри скінчених полів Галуа.

4. Розробка методів використання незворотних булевих перетворень для прискорення обчислювальної реалізації криптографічно строгої ідентифікації віддалених користувачів. Розробка методу строгої ідентифікації користувачів з використанням стандартизованих хеш-алгоритмів, за допомогою яких послідовність сеансових паролей формується користувачем у вигляді ланцюжка хеш-перетворень. Теоретична та експериментальна оцінка прискорення процесу ідентифікації в рамках теоретичної моделі “нульових знань” за рахунок використання стандартизованих хеш-перетворень.

5. Розробка та дослідження методу строгої ідентифікації віддалених користувачів на основі застосування для реалізації булевих незворотних перетворень стандартизованих шифроблоків, за допомогою яких користувачем формується послідовність сеансових паролей, перевірка правильності яких виконується системою в зворотному порядку. Теоретична та експериментальна оцінка ефективності реалізації незворотних булевих перетворень за допомогою стандартизованих шифроблоків для прискорення строгої ідентифікації користувачів.

6. Дослідження теоретичних і технологічних аспектів побудови незворотних неоднозначних булевих функціональних перетворень для прискореної строгої ідентифікації користувачів. Вибір структури обчислення таких перетворень та розробка методу їх синтезу. Дослідження залежності характеристик неоднозначних незворотних булевих перетворень від параметрів процедурної форми. Створення програмних засобів автоматизації проектування булевих функціональних перетворень спеціальних класів для ідентифікації абонентів на основі теоретичної концепції “нульових знань”.

7. Дослідження можливостей вдосконалення застосування незворотних перетворень в алгебрі полів Галуа для підвищення ефективності строгої ідентифікації користувачів за рахунок зменшення об'єму обчислень, необхідних для реалізації ідентифікації віддалених користувачів.

8. Розробка способу прискореного обчислення модулярної експоненти – базової операції строгої ідентифікації користувачів за рахунок організації паралельного виконання операцій модулярного піднесення до квадрату та модулярного множення,

Об'єкт дослідження – процеси строгої ідентифікації віддалених користувачів розподілених систем та обчислювальні процедури її реалізації з використанням незворотних перетворень булевої алгебри та алгебри скінчених полів Галуа.

Предмет дослідження – методи підвищення функціональної ефективності строгої ідентифікації користувачів за рахунок використання незворотних перетворень булевої алгебри та алгебри скінчених полів Галуа, програмні та апаратні засоби реалізації ідентифікації, в основі якої лежить теоретична концепція "нульових знань".

Методи дослідження базуються на теорії булевих функцій, комбінаторики, теорії ймовірностей, теоретичних положеннях криптографічної концепції "нульових знань", теорії організації обчислювальних процесів, а також на використанні методів моделювання.

Наукова новизна одержаних результатів полягає в наступному:

- Вперше запропоновано метод криптографічно строгої ідентифікації користувачів з застосуванням в якості сеансових паролей кодів, що утворюються в результаті послідовності хеш-перетворень з використанням стандартизованих хеш-алгоритмів, який дозволяє прискорити процес ідентифікації за рахунок того, що обчислювальна реалізація цих алгоритмів, основаних на незворотних булевих перетвореннях, виконується швидше в порівнянні з операціями модулярного експоненціювання в відомих методах строгої ідентифікації.

- Вперше запропоновано метод строгої ідентифікації віддалених користувачів на основі застосування стандартизованих шифроблоків, за допомогою яких користувачем формується послідовність сеансових паролей, перевірка правильності яких виконується системою в зворотному порядку, що дозволяє зменшити час ідентифікації користувача системою за рахунок того, що обчислювальна складність стандартизованих шифроблоків, основаних на незворотних булевих перетвореннях, на порядки менша складності операцій модулярного експоненціювання чисел великої розрядності.

- Вдосконалено метод прискореної строгої ідентифікації користувачів з використанням спеціальним чином побудованих незворотних булевих перетворень, які формують єдиний результат для множини сеансових

паролів, за рахунок застосування трапецевидної структури перетворювача зі зворотним зв'язком, що дозволяє зменшити ризик підбору пароля, збільшити кількість паролів та прискорити процес побудови перетворень.

- Вдосконалено метод використання для строгої ідентифікації користувачів незворотних перетворень на полях Галуа в частині використання властивостей локальних циклів експоненціювання на полях Галуа, утворюючий поліном яких є добутком двох простих поліномів різного ступеня, що дозволяє прискорити процес ідентифікації за рахунок того, що експоненціювання на полях Галуа виконується значно швидше в порівнянні з реалізацією цієї операції в традиційній алгебрі.

- Вперше запропоновано спосіб прискореного обчислення модулярної експоненти – базової операції строгої ідентифікації користувачів за рахунок організації паралельного виконання операцій модулярного піднесення до квадрату та модулярного множення, що дозволяє практично вдвічі прискорити обчислювальну реалізацію процесу строгої ідентифікації користувачів.

Практичне значення одержаних результатів роботи визначається можливістю значного прискорення (на 2-3 порядки) обчислювальної реалізації процедур строгої ідентифікації користувачів з використанням апаратних засобів, що дозволяє значно збільшити їх кількість а також підвищити рівень захищеності від атак типу перехоплення сеансу обміну даними. Використання стандартизованих, всебічно перевірених хеш-перетворень та шифроблоків для строгої ідентифиікації дозволяє підвищити рівень інформаційної безпеки та ефективно застосовувати апартно захищені високошвидкісні криптопроцесори, що випускаються серійно.

Результати роботи можуть бути застосовані для підвищення ефективності ідентифікації абонентів інтегрованих систем зберігання та обробки інформації в рамках глобальних та локальних компютерних мереж.

Особистий внесок здобувача полягає в теоретичному обґрунтуванні одержаних результатів, експериментальній їх перевірці та дослідженні, а також в створенні програмних продуктів для практичного використання одержаних результатів.

Всі результати, що наведені в дисертації отримані автором самостійно.

У роботах, що написані в співавторстві, автору належать: [2] – розробка способу реалізації строгої ідентифікації користувачів з використанням хеш-перетворень та шифроблоків; [3] – розробка способу паралельного обчислення модулярної експоненти; [4] – метод строгої ідентифікації користувачів з використанням алгебри полів Галуа; [5] – розробка теоретичних засад застосування незворотних неоднозначних булевих перетворень для реалізації строгої ідентифікації; [6] – обґрунтована можливість спрощення обчислювальних процедур строгої ідентифікації користувачів; [7] – аналіз ефективності використання хеш-перетворювачів для строгої

ідентифікації користувачів; [8] – ідея вдосконалення використання для прискорення ідентифікації перетворень на полях Галуа, [9] – спосіб конфігурування шифроблоків для генерації сеансових паролів користувачів.

Дисертаційна робота виконана на кафедрі обчислювальної техніки КПІ ім.. Ігоря Сікорського. Науковий керівник д.т.н., доцент Стіренко В.П.

Апробація результатів дисертації. Основні результати дисертації доповідались та обговорювались на 5 науково-технічних конференціях, з них 4 – міжнародних:

1. X Міжнародній науково-технічній конференції молодих вчених ”Електроніка - 2017”, 25-27 квітня 2017 р., м. Київ.

2. XI Міжнародній науково-технічній конференції ”Проблеми телекомунікацій”, 18-21 квітня 2017 р., м. Київ.

3. X Міжнародній науково-технічній конференції “Комп’ютерні системи та мережні технології”, 20-22квітня 2017 р., м. Київ.

4. IV Міжнародній науково-практичній конференції ”Summer Infocom Advanced Solution 2017”, 1-2 червня 2017 р., м. Київ.

5. IX Науковій конференції Прикладна математика та комп’ютинг ПМК-2017. Київ. 19-21 квітня 2017

Публікації. Основні положення дисертаційної роботи опубліковані в 9 наукових працях, серед яких 5 статей у наукових фахових виданнях (в тому числі 3 статті, що реферуються міжнародними наукометричними базами даних Index Copernicus, INSPEC IDEAS, EBSCO Publishing, DOAJ., 2 статі, що входять до наукометричної бази даних РІНЦ) та тез доповідей.

Структура та об’єм роботи. Дисертаційна робота складається з вступу, чотирьох розділів, висновків та додатків. Загальний обсяг роботи складає 143 сторінки, робота містить 12 рисунків, 7 таблиць та список використаної літератури на 95 найменувань, 2 додатки.

ОСНОВНИЙ ЗМІСТ

У вступі обґрунтована актуальність проблеми підвищення ефективності строгої ідентифікації користувачів розподілених комп’ютерних систем з огляду на зростання факторів ризику незаконного доступу до їх ресурсів та кількості користвачів. Ця проблема може бути вирішена шляхом розробки нових методів ідентифікації та створення якісно нових програмно-апаратних засобів, які забезпечать суттєве покращення характеристик ідентифікації в плані прискорення її обчислювальної реалізації та зниження ризику несанкціонованого доступу. Формулюються мета та задачі дослідження, визначені наукова новизна та практичне значення одержаних результатів.

У першому розділі дисертації виконано аналіз загроз несанкціонованого доступу до ресурсів розподілених систем обробки та зберігання інформації в

сучасних умовах, обґрунтувано на основі результатів аналізу, вимоги до процедур ідентифікації користувачів та критеріїв їх ефективності. Виконано огляд сучасного стану засобів ідентифікації користувачів розподілених систем та тенденцій їх розвитку з позицій сформульованих критеріїв.

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності, що досягається при її використанні та об'єм ресурсів, що застосовується для реалізації функцій захисту. Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, що намагається реалізувати незаконний доступ до ресурсів системи.

Всі сучасні протоколи ідентифікації абонентів розділяють на два класи: з використанням паролів, що перевіряються системою шляхом порівняння ("слабка" ідентифікація) та на основі теоретичної концепції "нульових знань" ("строга" ідентифікація).

Сутність цієї концепції полягає в тому, що для доведення своєї антентичності абонент має неявним чином виявити знання певної інформації, якою система не володіє, але може перевірити її наявність у абонента.

При цьому в системі не зберігається ніякої секретної інформації, яка дозволяє відновити ідентифікаційні дані абонента, що пояснює походження назви концепції "нульових знань". При кожному зверненні до системи абонентом генерується нова ідентифікуюча інформація.

Таким чином, концепція "нульових знань" найбільш повною мірою відповідає вимогам забезпечення високого рівня захищеності від спроб несанкціонованого доступу до ресурсів розподілених систем.

Концепція "нульових знань" базується на використанні незворотних математичних перетворень. В більшості існуючих схем строгої ідентифікації в якості таких перетворень використовуються аналітично нерозв'язувані задачі теорії чисел, зокрема відома задача дискретного логарифмування.

Найбільш відомими з схем ідентифікації цього класу є FFSIS (Feige Fiat Shamir Identification Scheme), методи Шнора (Schnorr) та Гіллоу-Квіскватера (Guillou- Quisquater). Базовими обчислювальними операціями для FFSIS є $A^2 \cdot B \bmod m$, а для методів Шнора і Гіллоу-Квіскватера - $A^e \cdot B^v \bmod m$.

З викладеного слідує, що базовою операцією більшості схем строгої ідентифікації віддалених абонентів є модулярне експоненціювання над числами, довжина яких значно перевищує розрядність процесору. В умовах стійкої тенденції до зростання розрядності чисел, обчислювальна складність реалізації вказаного типу операцій збільшується експоненційно, випереджаючи темпи зростання продуктивності комп'ютерних систем.

Таким чином, основний недолік існуючих методів строгої ідентифікації полягає в значній обчислювальній складності їх базових обчислювальних процедур. В сучасних умовах зростання кількості користувачів постає задача прискорення обчислювальної реалізації їх строгої ідентифікації.

Для вирішення цієї наукової задачі пропонується використати для реалізації строгої ідентифікації користувачів незворотні перетворення в альтернативних алгебра і, зокрема булевої алгебри та алгебри полів Галуа.

В другому розділі роботи досліджуються можливості використання для реалізації строгої ідентифікації незворотних булевих перетворень.

Незворотні булеві перетворення лежать в основі значної частини сучасних механізмів криптографічного захисту інформації: поточних шифрів, алгоритмів симетричного шифрування, хеш-перетворень. Властивість незворотності нелінійних булевих перетворень ґрунтується на тому, що не існує аналітичних методів розв'язання систем нелінійних булевих рівнянь. Основною перевагою використання незворотних булевих перетворень вважається висока швидкість обчислювальної реалізації.

Незворотні булеві перетворення можуть бути спеціальним чином побудовані користувачем, або реалізуватися існуючими хеш-алгоритмами типу SHA чи шифроблоками симетричного шифрування, які пройшли якісне тестування та перевірку практикою. Крім того, промисловістю випускається широкий спектр криптопроцесорів та криптоакселераторів, які на апаратному рівні реалізують стандартизовані блоки криптографічних перетворень.

Принципово існує дві можливості використання незворотних булевих перетворень: без зміни коду Y ідентифікації користувача, що зберігається в системі, і з його зміною при переході до наступного сеансу ідентифікації.

Якщо позначити через $\phi(p)$ перетворення, що виконується системою для ідентифікації користувача по його паролю p, то при незмінному коді Y ідентифікації користувача потрібно реалізувати таке булеве функціональне перетворення $\phi(p)$, для якого користувач може отримати сукупність паролів $p_1, p_2,\ldots,p_m \quad \forall p_j,\ j=1,2,\ldots,m$: $\phi(p_j) = Y$. Таке перетворення теоретично можна побудувати як хеш-перетворення з вбудованими колізіями. Система, маючи в розпорядженні незворотне перетворення $\phi(p)$ та вихідний вектор Y, не в змозі виконати зворотне перетворення, тобто отримати будь-який з кодів паролів $p_1, p_2,\ldots,p_m$ для яких $\phi(p_j) = Y$.

Інший варіант реалізації строгої ідентифікації полягає в тому, що код Y ідентифікації користувача змінюється при кожному зверненні його до системи. В найпростішому варіанті в якості коду Y ідентифікації користувача на поточному сеансі використовується попередній пароль користувача.

Такий варіант реалізації строгої ідентифікації пропонується виконувати з використанням стандартизованих хеш-перетворень.

Стандартизований хеш-перетворювач (H) – сертифікований відповідними органами алгоритм незворотного перетворення інформаційного блоку довільної довжини в код хеш-сигнатури фіксованої розрядності h. Найбільш відомими є хеш-перетворювачі SHA-1 та RIPEMD-160, що формують 160-бітову хеш-сигнатуру (h=160). На практиці застосовується також варіант хеш-перетворення збільшеної розрядності SHA-256 для якого h=256. Найважливішою якістю хеш-перетворювачів є їх незворотність – тобто практична неможливість віднаходження інформаційного блоку, хеш-сигнатура якого дорівнює заданій.

Пропонований метод регламентує процедури ініціалізації та сеансової ідентифікації при кожному зверненні абоненту до системи.

Метод передбачає таку послідовність дій при реєстрації :

1) Користувач довільно визначає кількість n циклів ідентифікації.
2) Випадковим чином генерує n–тий сеансовий пароль P_n.
3) Обчислює n-1 паролів, причому j-тий пароль P_j, j=n-1,…,0 обчислюється як хеш-перетворення H(x) від конкатенації попереднього паролю та номера сеансу: $P_j = H(P_{j+1} \| j)$.
4) Пароль P_0 відсилається в систему, зашифрований її відкритим ключем.

Послідовність дій j–того сеансу ідентифікації має вигляд:

1) Користувач шифрує відкритим ключем системи j-тий сеансовий пароль P_j і відсилає його в систему.
2) Система виконує хеш-перетворення над конкатенацією отриманого паролю та номера сеансу: $\xi = H(P_j \| j)$ і порівнює результату з попередньо отриманим паролем P_{j-1} : якщо $\xi = P_{j-1}$ то надається доступ.

Структура перетворень, що виконуються в запропонованому методі показана на рис.1

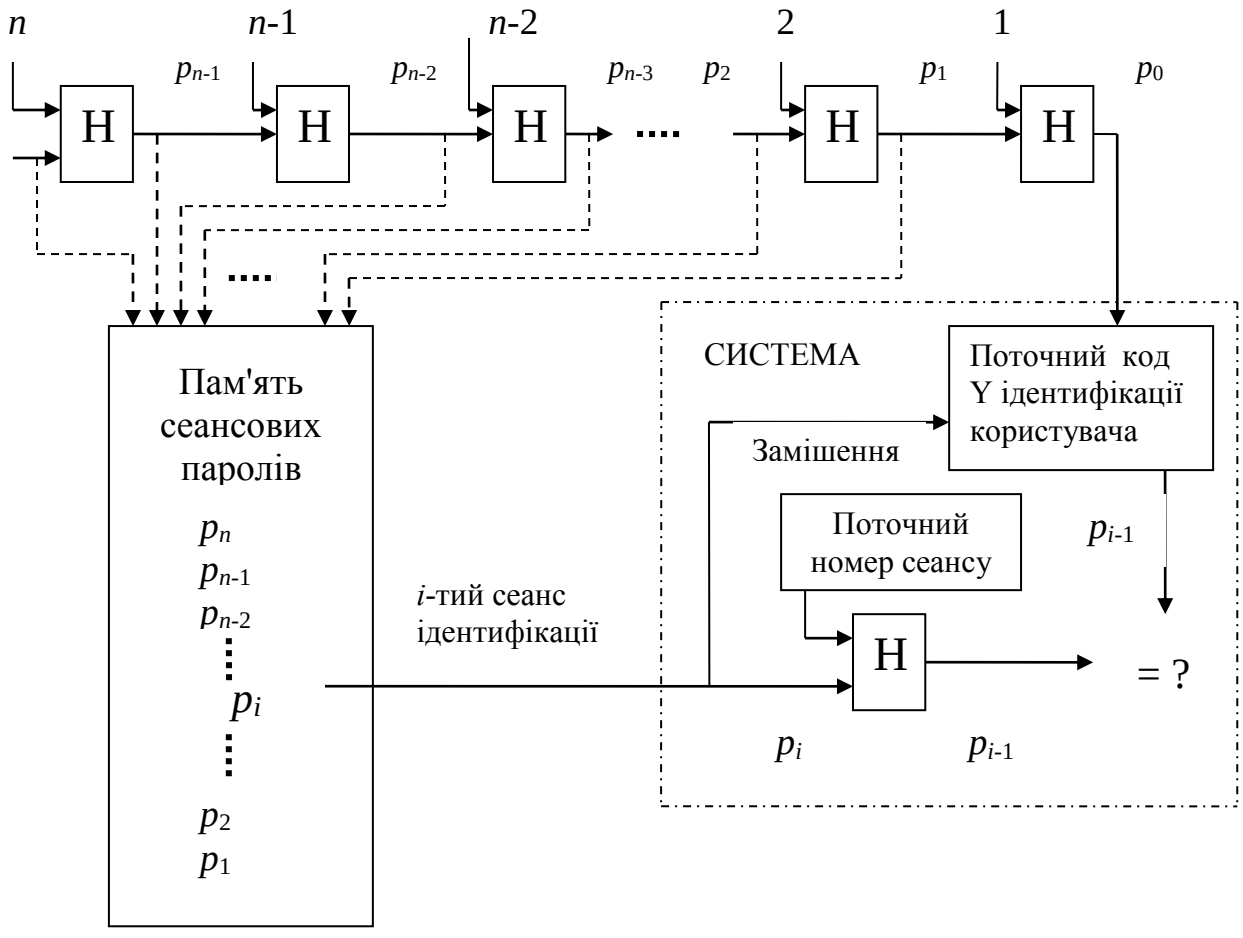

Рис.1. Структурна організація строгої ідентифікації з використанням ланцюжка хеш-перетворень

Очевидно, що система, маючи в розпорядженні попередній пароль P_{j-1} не здатна сама генерувати наступний пароль P_j : ця задача еквівалентна злому стандартизованого хеш-алгоритму. Використання стандартизованого

хеш-перетворення унеможливлює застосування для цього інших методів крім перебору. При цьому, в середньому, потрібно виконати 2^{h-1} прорахунків хеш-перетвореня, що для SHA-1 становить 2^{159} реалізацій алгоритму і виходить за рамки практичної доцільності.

Основною перевагою пропонованого методу є висока швидкість обчислювальної реалізації строгої ідентифікації системою, яка обслуговує в реальному часі сотні тисяч користувачів.

До недоліків методу слід віднести те, що всі сеансові паролі генеруватися користувачем відразу і зберігатися в пам'яті. Крім того, згенеровані користувачем паролі мають використовуватися строго послідовно, тобто жорстко прив'язані до номеру сеансу ідентифікації.

На основі запропонованого підходу розроблені більш складні методи строгої ідентифікації користувачів розподілених систем з використанням шифроблоків, а також шифроблоків і хеш-перетворювачів.

Стандартизований шифроблок (ШБ) являє сертифікований органами державної влади, алгоритм симетричного, тобто з використанням однакового ключа, шифрування-дешифрування блоку даних фіксованої довжини. До теперішнього часу найбільшого поширення набув шифроблок Rijndael, створений в рамках міжнародного проекту AES для заміни алгоритму шифрування першого покоління – DES.

В структурному плані шифроблок (ШБ) можна розглядати як функціональний перетворювач φ, на входи якого подаються m-розрядний блок D даних та k–розрядний ключ K, а на виході формується m–розрядний блок C зашифрованих даних: $C = \varphi(D,K)$. Відповідно, в режимі дешифрування шифроблок реалізує зворотне перетворення φ^{-1}: на його входи подаються $\boldsymbol{m}$-розрядний блок C зашифрованих даних та k–розрядний ключ K, а на виході відновлюється m-розрядний блок даних $D=\varphi^{-1}(C,K)$. Для шифроблоку AES регламентовано шифрування блоків, довжиною 128, 192 або 256 розрядів. В пропонованому методі використовується режим шифрування блоків довжиною 256 бітів (m = 256).

В останньому методі процедура ініціалізації включає два етапи:

1) Абонент випадковим чином формує d–розрядний двійковий код z, а також m–розрядний код R ідентифікатора абонента. Коди z та R в закритому режимі передаються в систему.

2) Абонент довільним чином обирає h-розрядний код q_n, після чого послідовно, з використанням стандартизованого хеш-перетворення H, обчислює n-1 h-розрядних кодів $q_{n-1}, q_{n-2},\ldots,q_2, q_1$ так, що кожен наступний з цих кодів являє собою хеш-сигнатуру попереднього, тобто, для кожного $i\in\{1,2,\ldots,n-1\}$: $q_i = H(q_{i+1})$. Сформовані таким чином коди зберігаються лише у абонента.

Процедура i–то сеансу ідентифікації абонента полягає у виконанні наступної послідовності дій:

1) Абонент формує m-розрядний код сеансового ключа K_i як конкатенацію –розрядного коду q_i та d-озрядного коду z: $K_i = q_i|z$.

2) Абонент формується m-розрядний код U_i як результат зворотного шифрування коду R ключем K_i : $U_i = \varphi^{-1}(R,K_i)$. Пара кодів q_i та U_i утворюють $(h+m)$-бітовий i-тий сеансовий пароль: $P_i = < q_i, U_i >$.

3) Сеансовий пароль P_i передається системі.

4) Система розділяє отриманий сеансовий пароль на складові q_i та U_i.

5) Перевіряється правильність отриманого коду q_i шляхом перевірки того, що результат хеш-перетворення q_i збігається з кодом q_{i-1} попереднього сеансу ідентифікації, тобто перевіряється умова: $q_{i-1} = H(q_i)$. Якщо ця умова не виконується, то сеанс ідентифікації переривається.

6) Система конкатенацією отриманого коду q_i та секретного коду z формує сеансовий ключ K_i : $K_i = q_i|z$.

7) З використання сеансового ключа система виконує пряме шифрування m-розрядного коду U_i : $Y=\varphi(U_i, K_i)$.

8) Якщо отриманий в результаті шифрування код Y дорівнює коду доступу R абонента, тобто $Y=R$, то ідентифікація абонента вважається успішною.

На рис.2 представлено структуру операцій, що виконуються при реєстрації користувача та при і-тому сеансі його ідентифікації.

Запропоновані процедури можуть бути доволі просто модифіковані для реалізації автентифікації віддалених користувачів розподілених систем.

Таким чином, метод забезпечує ідентифікацію користувачів з використанням паролей, що змінюються при кожному сеансі. При цьому система не здатна генерувати пароль, а може лише перевіряти його коректність.

Для аналізу ефективності запропонованих методів доцільно виконати їх оцінку за наступними критеріями:

- рівень захищеності від спроб отримати незаконний доступ до ресурсів системи як з боку сторонньої зловмисника, так і з боку осіб, що незаконно мають доступ до пам’яті системи;

- час обчислювальної реалізації процесу ідентифікації користувача;

В разі перехоплення послідовності паролей $P_1, P_2,\ldots,P_i$ стороннім зловмисником, його ціллю може бути відтвореня паролю P_{i+1} для наступного, $(i+1)$-го сеансу ідентифікації. Цей пароль складається з двох компонентів: h-розрядного коду q_{i+1} та m-розрядного коду U_{i+1}. Код q_{i+1} пов'язаний з кодом q_i попереднього сеансового пароля через співвідношення: $q_i = H(q_{i+1})$, тобто, для реконструкції q_{i+1} потрібно виконати зворотнє хеш-перетворення. Для стандартизованих хеш-перетворень єдиним методом реалізації зворотного перетворення є перебір. При цьому, в середньому, потрібно виконати 2^{h-1} прорахунків хеш-перетвореня, що для хеш-алгоритму SHA-1 становить 2^{159} реалізацій алгоритму і виходить за рамки практичної доцільності.

Найбільш вагома перевага запропонованих методів строгої ідентифікації в порівнянні з існуючими (схеми Fiat-Shamir, Schnorr) полягає в тому, що вони забезпечують значне проскорення процедури ідентифікації. Більшість існуючих методів строгої ідентифікації користувачів використовують

незворотні перетворення теорії чисел, базовою операцією яких є модулярне експоненціювання над числами великої розрядності.

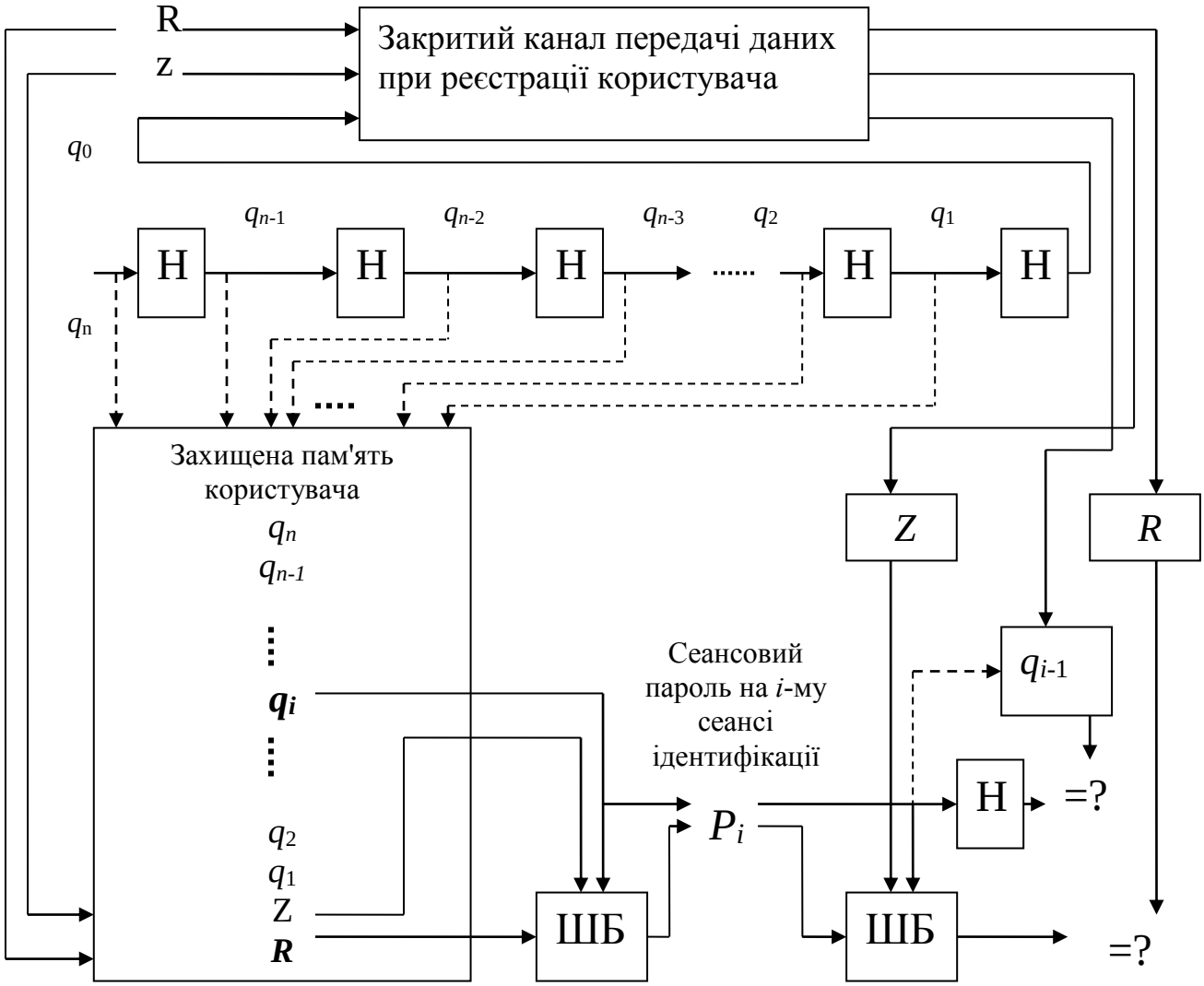

Рис.2. Структурна організація формування сеансових паролів, реєстрації та i-го сеансу ідентифікації користувача системою з використанням хеш-перетворювачів та шифроблоків

Для оцінки прискорення строгої ідентифікації, яке досягається розробленими методами розглянуто два варіанти реалізації: програмна та апаратна.

При програмній реалізації модулярного експоненціювання n-разрядних чисел на r–розрядному процесорі n-розрядні коди розділяються на k фрагментів ($k=n/r$). На сьогоднішній день найбільш ефективним алгоритмом модулярного експоненціювання вважається алгоритм Монтгомері, в якому для реалізації редукції використовується не ресурсоємка операція ділення, а простий зсув. Число операцій процесорного множення при використанні алгоритму Монтгомері дорівнює $3 \cdot n \cdot r(r+1)$, а число операцій додавання - $4 \cdot n \cdot r(r+1)$. Для сучасних процесорів операція додавання, зсуву виконуються за один машинний такт, а операція множення – за 10 тактів. Таким чином, загальна кількість T_M тактів для експонентціювання методом Монтгомері оцінюється як: $T_M = 34 \cdot n \cdot k \cdot (k-1)$.

Для реалізації шифроблоку AES-256 потрібно виконати 1430 логічних операцій XOR, 40 операцій зсуву, 320 операцій звернення до табличної пам’яті, що загалом становить 1720 процесорних команд.

На основі наведених даних проведені розрахунки кількості машинних тактів для реалізації AES-256 та модулярного експоненціювання. Результати розрахунків зведено в таблицю 1.

Табл. 1 Порівняльний аналіз часу програмної реалізації шифроблока AES-256 та операції модулярного експоненціювання

Розрядність чисел	Розрядність процесора	Кількість машинних тактів для реалізації модулярного експоненціювання	Співвідношення кількості машинних тактів для реалізації модулярного експоненціювання та шифроблоку
1024	32	36765696	5343
	64	9469952	1376
2048	32	289669120	21052
	64	73531392	5343

В сучасних умовах динамічного розвитку інтегральної технології невпинно збільшується питома вага виконання обчислень, пов’язаних з захистом інформації спеціалізованими апаратними засобами – крипто-процесорами або криптоакселераторів. Якщо в перші десять років нашого тисячоліття криптопроцесори входили до складу апаратного комплексу серверів, то нині сопроцесори підтримки криптографічних обчислень входять до складу більшості ноутбуків та навіть термінальних мікроконтролерів. Зокрема, всі мікроконтролери AVR родини XMega фірми Atmel оснащені криптоакселераторами шифроблоків DES і AES. Проведений аналіз ринку криптопроцесорів та криптоакселераторів показав, що в 100% з них апаратно реалізують шифроблоки DES або AES, 72% реалізують стандартизовані перетворення SHA і лише 42% виконують апаратну підтримку алгоритмів з відкритими ключами RSA або DSA.

З наведеного можна зробити наступні висновки:

- Використання запропонованих методів організації строгої ідентифікації на стандартизованих шифроблоках та хеш-перетворювачах дозволяє розшити сферу можливостей її апаратної швидкісної реалізації.

- Оцінка рівня прискорення обчислювальної реалізації строгої ідентифікації, що досягається запропонованими методами у порівнянні з традиційними може бути проведена шляхом порівняння часових характеристик реалізації стандартизованих шифроблоків AES та модулярного експоненціювання (алгоритму RSA) існуючими зразками криптопроцесорів.

Зокрема, фірмою Hi/fn випускаються криптопроцесори, що реалізують шифроблоки AES, стандартизовані перетворення SHA та алгоритм RSA. Характеристики сучасного криптопроцесора 7955 наведені в таблиці 2.

Табл 2. Часові характеристики криптопроцесора 7955 фірми Hi/fn

Криптографічний алгоритм	Швидкість шифрування Мбіт/с	
AES - 256	550	
SHA	325	
RSA	Час шифруваня мс	
	Розрядність 2048	Розрядність 1024
	82.75	11.88
	Оцінка прискорення обчислювальної реалізації строгої ідентифікації	
Співвідношення часу реалізації RSA та AES	22223	6380
Співвідношення часу реалізації RSA та SHA	13132	3775

Таким чином доведено, що при програмній і при апаратній реалізації застосування розроблених методів строгої ідентифікації дозволяє на декілька порядків прискорити обчислення, пов'язані з процедурою ідентифікації.

В третьому розділі роботи досліджуються теоретичні та практичні аспекти реалізації строгої ідентифікації з використанням незворотних перетворень на полях Галуа.

Досліджено циклічні властивості операції експоненціювання на полях Галуа, утворюючий поліном $M(x)$ яких являє собою поліноміальний добуток двох простих поліномів $d(x)$ та $g(x)$ з різними степенями v та u, відповідно.

Аналогічно тому, як у традиційній алгебрі в якості базової операції механізмів криптографічного захисту використовується модулярне експоненціювання $A^E \bmod M$, в алгебрі полів Галуа застосовується експонентціювання $A|^E \text{ rem } M$ на полях.

На практиці обчислення експоненти $R_1 = A|^E \text{ rem } M$ реалізується рекурсивною процедурою, яка для n-розрядної експоненти $E = e_1 + 2\cdot e_2 + 2^2\cdot e_3 + \ldots + 2^{n-1}\cdot e_n$, $e_1, e_2, \ldots, e_n \in \{0,1\}$ передбачає послідовне, починаючи з $R_n=1$ і $j=n$, обчислення значень $R_{n-1}, R_{n-2}, \ldots, R_1$ з використанням наступної формули:

$$R_{j-1} = (R_j \otimes R_j) \text{ rem } M \otimes (A\cdot e_j \oplus e_j \oplus 1) \text{ rem } M,$$

де символом '⊗' позначена операція поліноміального множення або множення без переносів (Multiplication Without Carry -MWC), а абревіатурою "rem" – операція редукції на полі Галуа, тобто віднаходження залишку при поліноміальному діленні на утворюючий поліном M поля.

Якщо $g(x)$ – простий поліном ступеню d, то для будь-якого $u(x)$, що є елементом поля $GF(2^d)$ і якому співвідноситься d-розрядне двійкове число u, таке, що $0 < u \le h$, де $h=2^d-1$ виконується $u|^{h+1} \; rem \; g = u$.

Теоретично доведено, що якщо утворюючий поліном $M(x)$ ступеню r являє собою добуток двох простих поліномів $p(x)$ ступеню v і $g(x)$ ступеню d : $M(x)=p(x)\otimes g(x)$, $r = v+d$, причому поліному $M(x)$ співвідноситься двійкове число m, то для будь-якого $u(x)$, що належить полю $GF(2^v)$ і з яким

співвідноситься число u, $u \le h=2^d-1$ справедливо: $(u \otimes p)|^{h+1} \; rem \; m = u \otimes p$. Аналогічно, для будь-якого поліному $w(x)$, що належить полю GF(2^d) та співвідноситься з числом w, так, що $w \le l=2^v-1$ справедливо: $(w \otimes g)|^{l+1} \; rem \; m = w \otimes g$

Базуючись на встановленій властивості пропонується метод ідентифікації віддалених користувачів, який реалізує строгу ідентифікацію.

Процедура реєстрації передбачає наступну послідовність дій:

1) Користувач отримує від системи її відкритий закриваючий ключ $К_с$.

2) Користувач довільним чином вибирає пару простих поліномів $p(x)$ та $g(x)$ з різними степенями: $p(x)= x^v + p_{v-1}\cdot x^v + \ldots + + p_1 \cdot x + p_0$ степені v та $g(x)= x^d + g_{d-1}\cdot x^{d-1} + + \ldots + g_1 \cdot x + g_0$ степені d, де $p_0, p_1, \ldots, p_{v-1} \in \{0,1\}$, $g_0, g_1, \ldots, g_{d-1} \in \{0,1\}$, причому $d > v$.

3) Користувач формує поліном $M(x)$ у вигляді поліноміального добутку вибраних двох поліномів $p(x)$ та $g(x)$: $M(x) = p(x) \otimes g(x)$. Число m, з яким співвідноситься поліном $M(x)$ являє собою першу компоненту відкритого ключа користувача.

4) Користувач вибирає випадкове число β: $0 < \beta < 2^d$ та обчислює другу компоненту α відкритого ключа користувача у вигляді: $\alpha = p \,|^{\beta} \text{ rem } m$.

5) Обидві компоненти відкритого ключа користувача: m та β шифрують ся відкритим закриваючим ключем $К_с$ і відсилаються системі.

6) Система з використанням секретного відкриваючого ключа $К_о$ відновлює значення обох компонентів m і β ключа користувача після чого зберігає їх в захищеній пам'яті.

Запропонована процедура сеансу ідентифікації передбачає виконання наступної послідовності дій:

1) Користувач довільним чином вибирає число k менше за 2^d. Виконується поліноміальне множення відповідного числу k поліному $k(x)$ на поліном $p(x)$: $q(x) = = k(x) \otimes p(x)$.

2) Користувач довільним чином вибирає число $U < 2^d$ та виконує експоненціювання на полі Галуа з базовим поліномом $M(x)$: $R = q|^U \text{ rem } M$.

3) Користувач обчислює $E = 2^u - U$ і надсилає в систему трійку чисел $<q, R, E>$, які утворюють сеансовий пароль користувача.

4) Система отримує від користувача сеансовий пароль у вигляді трійки чисел $< q, R, E >$, обчислює $\rho = q|^E \text{ rem } M$ шляхом піднесення q до степеня E в полі Галуа з базовим поліномом $M(x)$. Далі системою обчислюється добуток в полі Галуа: $\eta = \rho \otimes R \text{ rem } M$. Отриманий результат η порівнюється з q: якщо $\eta = q$, то ідентифікація користувача вважається успішною.

Основна перевага запропонованого способу строгої ідентифікації користувачів полягає в тому, що використання експоненціювання в полях Галуа дозволяє значно прискорити час виконання програм та спростити апаратну реалізацію. Нижче наведені основні чинники, які дозволяють прискорити програмну реалізацію незворотних перетворень на полях Галуа в

порівнянні з мультиплікативними перетвореннями модулярної арифметики, що лежать в основі існуючих методів:

- операція піднесення числа до квадрату, питома вага якої складає 75% об'єму обчислень, на полях Галуа зводиться до вставки нулів між бітами числа, тобто не потребує ніяких обчислювальних операцій. В той же час операція модулярного піднесення до квадрату n-розрядного числа в традиційній алгебрі потребує виконання $(n/m)^2/2$ операцій процесорного множення;

- при виконанні операцій на полях Галуа кожен розряд оброблюється незалежно від інших: це дає змогу ефективно організувати розпаралелювання обчислювального процессу, особливо при використанні апаратних засобів;

- операції на полях Галуа не використовують міжрозрядних переносів, формування яких при розрядностях 2018 і 4096 потребує помітних затрат часових та апаратних ресурсів.

В четвертому розділі роботи розроблено теоретичні та практичні аспекти прискорення строгої ідентифікації користувачів при використанні незворотних перетворень в традиційній алгебрі. Запропоновано метод прискореної ідентифікації, а також спосіб прискореного обчислення модулярної експоненти. Використання розроблених новацій дозволяє прискорити процес строгої ідентифікації приблизно в 1.8 разів.

ВИСНОВКИ

В дисертаційній роботі, відповідно до поставленої мети, виконано теоретичне обґрунтування і одержано нове вирішення наукової задачі: підвищення ефективності строгої ідентифікації користувачів розподілених систем за рахунок прискорення її обчислювальної реалізації.

Основні наукові і практичні результати полягають у наступному.

1. Виконано аналіз сучасного стану механізмів захисту від несанкціонованого доступу до ресурсів розподілених систем. Доведено, що при сучасних можливостях доступу широкого кола користувачів до значних за обсягом обчислювальних ресурсів, які потенційно можуть бути використані для підбору паролей, надійний захист може бути забезпечений лише при застосуванні строгої ідентифікації в рамках моделі "нульових знань".

2. Проведений огляд існуючих механізмів строгої ідентифікації користувачів показав, що в їх основі лежить використання ресурсоємких операцій модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесорів, що зумовлює низьку швидкість обчислювальної реалізації ідентифікації користувачів. В сучасних умовах зростання їх кількості ключовою задачею практичного використання моделі строгої ідентифікації є підвищення швидкодії її обчислювальної реалізації.

3. Проведений аналіз можливостей прискорення обчислювальної реалізації строгої ідентифікації показав, що найбільш перспективним рішенням є застосування незворотних перетворень на альтернативній алгебраїчній

основі, обчислювальна реалізація яких потребує менших обчислювальних ресурсів в порівнянні з модулярним експоненціюванням.

4. Теоретично обґрунтована можливість застосування для строгої ідентифікації користувачів незворотних булевих перетворень. В рамках реалізації цієї можливості розроблено метод криптографічно строгої ідентифікації користувачів з застосуванням в якості сеансових паролей кодів, що утворюються в результаті послідовності хеш-перетворень з використанням стандартизованих хеш-алгоритмів, який дозволяє прискорити процес ідентифікації за рахунок того, що обчислювальна реалізація цих алгоритмів, основаних на незворотних булевих перетвореннях, виконується швидше в порівнянні з операціями модулярного експоненціювання в відомих методах строгої ідентифікації. Використання стандартизованих, всебічно перевірених хеш-перетворень дозволяє зменшити ризики несанкціонованого доступу до ресурсів розподілених систем і використовувати крипто-процесори, які серійно випускаються в мають вбудовані апаратні засоби реалізації стандартизованих хеш-перетворень.

5. Обґрунтовано, розроблено та досліджено метод строгої ідентифікації віддалених користувачів на основі застосування стандартизованих шифроблоків, за допомогою яких користувачем формується послідовність сеансових паролей, перевірка правильності яких виконується системою в зворотному порядку, що дозволяє зменшити час ідентифікації користувача системою за рахунок того, що обчислювальна складність шифроблоків, основаних на незворотних булевих перетвореннях, на порядки менша склад-ності операцій модулярного експоненціювання чисел великої розрядності.

6. Вдосконалено метод прискореної строгої ідентифікації з використанням спеціальним чином побудованих незворотних булевих перетворень, які формують єдиний результат для множини сеансових паролів, за рахунок застосування трапецевидної структури перетворювача зі зворотним зв’язком, що дозволяє зменшити ризик підбору пароля, збільшити кількість паролів та прискорити процес побудови перетворень. Розроблено спосіб формування незворотного булевого функціонального перетворення в процедурній формі.

7. Теоретично досліджено властивості локальних циклів, що утворюються при виконанні експоненціювання на полях Галуа, утворюючий поліном якого являє собою добуток двох простих поліномів різного ступеня. На основі виявлених та доведених властивостей запропоновано метод строгої ідентифікації користувачів з використанням незворотних перетворень на полях Галуа. Теоретично та експериментально доведено, що використання методу дозволяє прискорити на 1-2 порядки обчислювальну реалізацію строгої ідентифікації відомими методами.

8. На основі дослідження процедури модулярного експоненціювання запро-поновано спосіб прискореного обчислення модулярної експоненти за рахунок організації паралельного виконання операцій модулярного

піднесення до квадрату та модулярного множення, що дозволяє в 1.8 раз прискорити обчислювальну реалізацію строгої ідентифікації користувачів.

9. Розроблено програмні засоби прискореної строгої ідентифікації користувачів розподілених систем, що реалізують запропоновані методи.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Захариудакис Лефтерис. Метод быстрой аутентификации удаленных пользователей на основе концепции “нулевых знаний” /Наукові записки Українського науково-дослідного інституту зв’язку. 2017.- № 1 (45).– С.109-117. (Входить до міжнародної наукометричної бази РІНЦ - Російського індексу наукового цитування).

2. Марковський О. П. Метод строгої ідентифікації віддалених абонентів на основі стандартизованих шифроблоків та хеш-перетворень / О.П. Марковський, Захаріудакіс Лефтеріс., М.Ф. Федотов // Вісник Національного технічного університету України “КПІ” Інформатика, управління та обчислювальна техніка. К.: ТОО „ВЕК+”. 2016.- № 64.- С. 161-165. (Входить до міжнародної наукометричної бази DOAJ -Directory of Open Access Journals, а також до бази РІНЦ - Російського індексу наукового цитування). - *Автору належить розробка способу реалізації строгої ідентифікації користувачів з використанням хеш-перетворень та шифроблоків*.

3. Стіренко С.Г. Спосіб прискореного обчислення модулярної експоненти / С.Г. Стіренко О.П. Марковський, Захаріудакіс Лефтеріс., Л.Д. Міщенко // Вісник Національного технічного університету України “КПІ” Інформатика, управління та обчислювальна техніка. К.: ТОО „ВЕК+”.2017.- № 65.- С. 110-115. (Входить до міжнародної наукометричної бази DOAJ -Directory of Open Access Journals, а акож до бази РІНЦ - Російського індексу наукового цитування) - *Автору належить спосіб паралельного обчислення модулярної експоненти.*

4. Марковський О. П. Використання алгебри полів Галуа для реалізації концепції нульових знань при ідентифікації та автентифікації віддалених користувачів /О.П.Марковський, Захаріудакіс Лефтеріс., В.Р.Максимук // Электронное моделирование. 2017.- № 6.- С.96-110. (Реферується наукометричними базами Україніка наукова, Index Copernicus, INSPEC IDEAS (Institution of Engineering and Technology, Великобританія) – *Автору належить метод строгої ідентифікації користувачів з використанням алгебри полів Галуа.*

5. Мухін В.Є. Метод ідентифікації віддалених абонентів на основі концепції “нульових знань” / В.Є. Мухін, Лефтеріс Захаріудакіс, Ю.Н. Герасименко, М.С. Козерацький // Телекомунікаційні та інформаційні технології, 2017 – №1.– С.50-57. (Входить до міжнародної наукометричної бази РІНЦ - Російського індексу наукового цитування). – *Автору належить розробка теоретичних засад застосування незворотних неоднозначних булевих функціональних перетворень для реалізації строгої ідентифікації*

6. Марковський О.П. Метод строгої ідентифікації абонентів в телекомунікаційних системах / О.П. Марковський, Лефтеріс Захаріудакіс, М.Ф. Федотов // XI Міжнародна науково-технічна конференція “Проблеми телекомунікації” ПТ-2017: Збірник матеріалів конференції.К.:КПІ ім. Ігоря Сікорського, 2017.- С.334-337. – *Автором обґрунтована можливість спрощення обчислювальних процедур строгої ідентифікації користувачів*

7. Марковський О.П. Метод швидкої строгої ідентифікації віддалених користувачів / О.П. Марковський, Лефтеріс Захаріудакіс, М.Ф. Федотов // X Міжнародна науково-технічна конференція “Комп’ютерні системи та мережні технології” : Тези доповідей.К.: НАУ, 2017.- С. 59-61. – *Автором виконано аналіз ефективності використання хеш-перетворювачів для строгої ідентифікації користувачів*.

8. Захаріудакіс Лефтеріс Метод строгої ідентифікації віддалених користувачів з використанням перетворень на полях Галуа / Захаріудакіс Лефтеріс, А.А.Олієвський // IV Міжнародна науково-практична конференція ”Summer Infocom Advanced Solution 2017”,: Збірник матеріалів конференції. К.:КПІ ім. Ігоря Сікорського, 2017.- С.56-60. – *Автору належить ідея вдосконалення використання для прискорення ідентифікації перетворень на полях Галуа* .

9. Марковський О.П. Метод строгої ідентифікації абонентів з використанням шифроблоків / О.П. Марковський, Захаріудакіс Лефтеріс, Д.В. Горст // Збірник тез доповідей 9-ї наукової конференції Прикладна математика та комп’ютинг ПМК-2017. Київ 19-21 квітня 2017. – К.:Просвіта, 2017 – С.190-194. – *Автору належить спосіб конфігурування шифроблоків для генерації сеансових паролів користувачів*.

АНОТАЦІЇ

Захаріудакіс Лефтеріс. Методи та засоби підвищення ефективності ідентифікації користувачів розподілених систем. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп’ютерні системи та компоненти. – Національний технічний університет України ”Київський політехнічний інститут імені Ігоря Сікорського”, Київ, 2017.

Дисертація присвячена проблемі підвищення ефективності ідентифікації користувачів розподілених систем за рахунок зниження ризику несанкціонованого доступу до її ресурсів та прискорення ідентифікації.

В роботі проведено аналіз факторів. що впливають на ефективність ідентифікації віддалених користувачів інтегрованих систем. Основну увагу приділено підвищенню продуктивності ідентифікації.

З теоретичної точки зору найбільший рівень протидії незаконному доступу до ресурсів системи забезпечується при використанні строгої ідентифікації, в основі якої лежить модель “нульових знань” і яка передбачає використання математичних незворотних перетворень. В дисертаційній

роботі пропонується для прискорення строгої ідентифікації використовувати незворотні перетворення булевої алгебри та алгебри полів Галуа.

Для строгої ідентифікації на основі незворотних булевих перетворень пропонується три методи. Перший із них передбачає використання спеціально побудованого перетворення, яке формує однакових вихідний код для групи різних вхідних кодів.

Інший розроблений метод реалізації строгої ідентифікації з використанням булевих перетвореннях базується на застосуванні стандартизованих хеш-алгоритмів таких як SHA чи Ripemd-160. Третій метод для прискореної строгої ідентифікації на булевих перетвореннях передбачає використання стандартизованих шифроблоків типу AES.

Для всіх трьох з запропонованих методів розроблено процедури реєстрації користувачів і сеансу ідентифікації. Теоретично та експериментально доведено, що використання незворотних булевих перетворень замість моулярного експоненціювання дозволяє прискорити процес ідентифікації на два порядки в порівнянні з існуючими методами.

Запропоновано метод реалізації строгої ідентифікації віддалених користувачів з використанням незворотних перетворень на полях Галуа. Досліджено циклічні властивості експоненціювання на полях Галуа спеціальних класів. На основі цих властивостей запропоновано процедури реєстрації та ідентифікації користувачів. Теоретично та експериментально доведено, що запропонований підхід забезпечує прискорення процесів ідентифікації на 1-2 порядки при апаратній реалізації.

Ключові слова: строга ідентифікація, ідентифікація на основі концепції “нульових знань”, незворотні перетворення, шифр блоки, хеш-алгоритми.

Zacharioudakis Eleftheris. Methods and tools for increasing the efficiency of distributed systems users identifications. - Manuscript.

Thesis for a Ph.D. degree by specialty 05.13.05 – Computer system and components. National Technical University of Ukraine “Igor Sykorsky Kiev Polytechnic Institute”, Kiev, 2017.

Thesis is dedicated to a problem of increasing of efficiency of distributed systems users identifications by impairsing the risk of illegal access to system resources and by speed up identification.

In this work the analysis the factors which affect on efficiency of identification of remote user of integrate systems have been workwed out. The main attention is concentrated to identification performance increase.

From the theoretical point of view the best for high degree of safety again illegal access to system resources is zero-knowledge or strikt identification, based on utilization of nonreversable mathematical transformation. In dissertation work proposed for speed up strikt identification to use nonreversable transformation of boolean algebra and Galoise fields algebra.

For strikt identification based on nonreversable boolean transformation the three method have been proposed. Fist of them provision utilization special

building transformation which formed one output code for groop different input code. Another diveloped method strikt identification implementation by nonreversable boolean transformation are based on using standard hash-algorithms lile SHA or Ripemd-160. Third proposed method for strict identification by using boolean transformation is based on using of standard block ciphers such as AES.

For all three metdod the procedures for user registration and for the execution of a round of identification have been worked out. Theoretical and experimental evaluation have demonstrated that utilisation nonreversable boolean transformation instead modular exponentation achieves an acceleration of the identification process by two orders of magnitude, compared to existing schemes.

The method for implementation of strict remote users identification and authentication by using nonreversible Galois field transformation has been developed. The cyclic properties of special class Galois field exponentiation have been theoretically investigated. Based on those properties the procedures of user registration and user identification procedures have been proposed. It is shown, both theoretically and experimentally that the proposed approach provides of acceleration user identification process by 1 –2 orders of magnitude, via a hardware implementation.

Key words: strict identification, zero-knowledge identification, nonreversable transformation, block ciphers, hash algorithms.

Захариудакис Лефтерис. Методы и средства повышения эффективности идентификации пользователей распределенных систем. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – Компьютерные системы и компоненты. - Национальный технический университет Украины ”Киевский политехнический институт имени Игоря Сикорского”, Киев, 2017.

Диссертация посвящена проблеме повышения эффективности идентификации пользователей распределенных систем за счет снижения риска несанкционированного доступа к ее ресурсам и повышения скорости идентификации.

В работе проведен анализ факторов, влияющих на эффективность идентификации удаленных пользователей интегрированных систем. Основное внимание уделено повышению производительности идентификации.

С теоретической точки зрения наибольший уровень противодействия несанкционированному доступу к ресурсам систем обеспечивается при использовании строгой идентификации, в основе которой лежит модель “нулевых знаний” и которая предполагает использование математически необратимых преобразований. Известные методы реализации строгой идентификации не способны обеспечить высокую скорость ее вычислительной реализации в силу того, что в качестве указанных

преобразований используется модулярное экспоненцирование, выполняемое над числами большой разрядности.

В диссертационной работе предлагается для ускорения вычислительной реализации строгой идентификации использовать необратимые преобразования булевой алгебры и алгебры полей Галуа.

Для строгой идентификации на основе необратимых булевых преобразований предлагается три метода. Первый из них предусматривает использование специально построенного преобразования, которое формирует единый выходной сигнал для группы разных входных сигналов. Разработана технология получения такого преобразования.

Другой разработанный метод реализации строгой идентификации с использованием необратимых булевых преобразований базируется на применении стандартизированных хеш-алгоритмов типа SHA или Ripemd-160. Третий из предложенных методов ускоренной строгой идентификации на необратимых булевых преобразованиях предусматривает использование стандартизированных шифроблоков типа AES.

Для всех трех из предложенных методов разработаны процедуры регистрации пользователей и сеанса их идентификации. Теоретическими и экспериментальными исследованиями показано, что использование необратимых булевых преобразований позволяет ускорить вычислительную реализации процесса идентификации на два порядка по сравнению с существующими методами. Анализ возможностей аппаратной реализации показал возможность достижения существенно большего выиграша в скорости идентификации – на 3-4 порядка.

Предложен метод реализации строгой идентификации удаленных пользователей с использованием необратимых преобразований на полях Галуа. Исследованы циклические свойства операции возведения в степень на полях Галуа специальных классов. На основе этих свойств разработаны процедуры регистрации и идентификации пользователей, функционирование которых иллюстрировано числовыми примерами. Теоретически и экспериментально показано, что предложенный подход позволяет ускорить процедуру идентификации на один-два порядка при аппаратной реализации.

Предложен способ ускорения базовой вычислительной операции существующих методов строгой идентификации – модулярного экспоненцирования, основанный на параллельном выполнении операций модулярного возведения в квадрат и модулярного умножения. Доказано, что предложенный способ позволяет ускорить вычисление модулярной экспоненты в 1.8 раза.

Ключевые слова: строгая идентификация, идентификация на основе концепции “нулевых знаний”, необратимые преобразования, шифроблоки, хеш-алгоритмы.