SCI-CONF.COM.UA

EURASIAN SCIENTIFIC CONGRESS

ABSTRACTS OF XI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE NOVEMBER 1-3, 2020

BARCELONA 2020

EURASIAN SCIENTIFIC CONGRESS

Abstracts of XI International Scientific and Practical Conference

Barcelona, Spain

1-3 November 2020

Barcelona, Spain

2020

UDC 001.1

The 11th International scientific and practical conference "Eurasian scientific congress" (November 1-3, 2020) Barca Academy Publishing, Barcelona, Spain. 2020. 613 p.

ISBN 978-84-15927-31-0

The recommended citation for this publication is:
Ivanov I. Analysis of the phaunistic composition of Ukraine // Eurasian scientific congress. Abstracts of the 11th International scientific and practical conference. Barca Academy Publishing. Barcelona, Spain. 2020. Pp. 21-27. URL: https://sci-conf.com.ua/xi-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiya-eurasian-scientific-congress-1-3-noyabrya-2020-goda-barselona-ispaniya-arhiv/.

Editor
Komarytskyy M.L.
Ph.D. in Economics, Associate Professor

Collection of scientific articles published is the scientific and practical publication, which contains scientific articles of students, graduate students, Candidates and Doctors of Sciences, research workers and practitioners from Europe, Ukraine, Russia and from neighbouring coutries and beyond. The articles contain the study, reflecting the processes and changes in the structure of modern science. The collection of scientific articles is for students, postgraduate students, doctoral candidates, teachers, researchers, practitioners and people interested in the trends of modern science development.

e-mail: barca@sci-conf.com.ua

homepage: *https://sci-conf.com.ua*

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Карпанасюк Віктор Володимирович
Магістр
Пасічник Олександр Анатолійович
к.т.н., доцент
Хмельницький національний університет
м. Хмельницький, Україна

Вступ./Introductions. Основною рушійною силою технологічного прогресу людства в останні десятиліття є активна інтеграція інформаційних систем та утворення інформаційного простору, в якому надається доступ до великих обсягів приватної та конфіденційної інформації як до підґрунтя прийняття оптимальних рішень. Використання таких систем може бути доцільним та раціональним лише за умови ефективного вирішенням питання ідентифікації віддалених користувачів.

Мета роботи./Aim. Мета роботи полягає у розробці інформаційної технології, яка буде надійно захищати різноманітні системи від протиправного доступу шляхом ідентифікації користувачів на основі криптографічної концепції нульових знань.

Матеріали и методы./Materials and methods. Базовою складовою будь-яких інформаційних систем є модулі захисту, які виконують ідентифікацію користувачів, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами систем. Слід зазначити, що як суб'єкти систем можуть виступати як користувачі, так і процеси, а я об'єкти - інформація та інші інформаційні ресурси системи.

Присвоєння суб'єктам і об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією.

Ідентифікація забезпечує виконання таких функцій:

- встановлення автентичності та визначення повноважень суб'єкта при

його допуску в систему;

- контроль встановлених повноважень в процесі сеансу роботи;

- реєстрація дій тощо.

Одними з найпоширеніших технологій ідентифікації користувачів є технології, засновані на знанні особою, яка має право на доступ до ресурсів системи, деякою секретної інформації, наприклад, пароля. Такі методи ідентифікації є найбільш поширеними, простими і звичними. Парольні методи класифікують за ступенем частоти змінюваності паролів на методи з постійними (багаторазовими) або динамічно змінюваними (одноразовими) паролями.

У більшості систем використовуються багаторазові паролі, хоча більш надійним є спосіб з використанням одноразових або динамічно змінюваних паролів. Існують такі методи парольного захисту, засновані на одноразових паролів: - методи модифікації схеми простих паролів; - методи «запит-відповідь»;

До методів модифікації схеми простих паролів відносять випадкову вибірку символів пароля і одноразове використання паролів.

При використанні методу модифікації простих паролів, кожному користувачеві виділяється досить довгий пароль, причому щоразу для ідентифікації використовується не весь пароль, а тільки його деяка частина. У процесі перевірки автентичності система запитує у користувача групу символів під заданим порядковим номерам. Кількість символів і їх порядкові номери для запиту визначаються за допомогою датчика псевдовипадкових чисел.

При одноразовому використанні паролів кожному користувачеві виділяється список паролів. В процесі запиту номер пароля, який необхідно ввести, вибирається послідовно за списком або по схемі випадкової вибірки.

Недоліком методів модифікації схеми простих паролів є необхідність запам'ятовування користувачами довгі паролі або їх списки. Запис же паролів на папір або в записники призводить до появи ризику втрати або розкрадання носіїв інформації з записаними на них паролями.

При використанні методу «запит-відповідь» система задає користувачеві деякі питання загального характеру, правильні відповіді на які відомі тільки конкретного користувача.

Відзначимо, що методи ідентифікації, засновані на одноразових паролях, також не забезпечують абсолютного захисту. До прикладу, якщо зловмисник має можливість підключення до мережі і перехоплювати передані пакети, то він може посилати останні як власні.

Базовими критеріями ефективності будь-якої системи захисту є рівень захищеності при її використанні та обсяг ресурсів для реалізації функцій захисту. Складність проблеми визначається неможливістю побудови адекватної формальної моделі дій сторони, яка 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),

- на основі концепції “нульових знань” (“сурова” ідентифікація).

Сутність концепції “нульових знань” полягає в тому, що для доведення своєї ідентичності 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 жодних секретних даних, які б дозволили б відновити ідентифікаційні дані абонента "нульових знань”. Під час кожного зверненні до системи генерується нова ідентифікуюча інформація. Таким чином, концепція “нульових знань” найбільш повною мірою задовольняє вимогам забезпечення високого рівня захищеності від спроб несанкціонованого доступу.

Концепція “нульових знань” ґрунтується на використанні незворотних математичних перетворень. В більшості існуючих схем строгої ідентифікації як такі перетвореньня 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-Квіскатера (Guillou- Quisquater).

Важливою передумовою взаємодії віддалених користувачів та інформаційних систем є наявність ефективних механізмів контролю доступу до інформаційних ресурсів. Як основа існуючих методів ідентифікації використовуються операції модулярної арифметики з числами розрядність яких значно перевищує розрядність процесорів й, відповідно, потребують суттєвих обчислювальних витрат.

Розширення спектру та обсягів інформації широкого кола користувачів, що зберігається у цифровому форматі, обумовлює об'єктивну зацікавленість певних «недоброзичливців» в отриманні доступу до неї в обхід законних процедур. Разом із тим, система ідентифікації не повинна створювати незручності, зокрема, збільшення часу очікування для отримання доступу, для доброчесних користувачів.

Таким чином, розробка нових підходів до підвищення швидкості програмної та апаратної реалізації базових обчислювальних процедур в методах ідентифікації є актуальною проблемою. Для її вирішення пропонується як основа для обчислювальних процедур методів ідентифікації, використовувати алгебру кінцевих полів Галуа з реалізація операції експоненціювання.

Для ефективної організації експоненціювання на кінцевих полях важливе значення має специфічна властивість поліноміального квадрату, а саме - двійкові розряди поліноміального квадрату числа А, що знаходяться на парних позиціях дорівнюють нулю, в той час, як розряди з непарними номерами співпадають з двійковими розрядами числа А, тобто, якщо $A=a_0+a_1\cdot 2+a_2\cdot 2^2+...+a_{n-1}\cdot 2^{n-1}$, то $A\otimes A=A|^2 = a_0+a_1\cdot 2^2+a_2\cdot 2^4+...+a_{n-1}\cdot 2^{2\cdot n-2}$.

Поліноміальне представлення числа A має вигляд $P(A) = a_{n-1}\cdot x^{n-1} + a_{n-2}\cdot x^{n-2} + ... + a_1\cdot x + a_0$. Відповідно, поліноміальне представлення квадрату $A\otimes A$ числа А має наступний вигляд: $P(A\otimes A) = b_{2\cdot n-2}\cdot x^{2\cdot n-2} + b_{2\cdot n-3}\cdot x^{2\cdot n-3} + ... + b_3\cdot x^3 + b_2\cdot x^2 + b_1\cdot x + b_0$. Кожен коефіцієнт $b_l \in\{0,1\}$, де $l\in\{0,1,...,2\cdot n-2\}$ поліноміального представлення квадрату $P(A\otimes A)$ дорівнює сумі попарних добутків коефіцієнтів $a_q\cdot a_g$ таких, що арифметична сума їх індексів дорівнює l: $q+g=l$; наприклад, b_0 =

$a_0 \cdot a_0$, $b_1 = a_1 \cdot a_0 + a_0 \cdot a_1$ $b_1 = a_2 \cdot a_0 + a_0 \cdot a_2 + a_1 \cdot a_1$. Очевидно, якщо $g \neq q$, то до складу вказаної суми входять обидва коефіцієнти $a_q \cdot a_g$ та $a_g \cdot a_q$, а якщо $g = q$, то лише один: $a_q \cdot a_g$. Оскільки $a_q \cdot a_g = a_g \cdot a_q$ то, в алгебрі кінцевих полів вони при додаванні взаємно компенсуються. Тобто, для непарних значень l коефіцієнт $b_l = 0$, а для парних значень l коефіцієнт $b_l = a_{l/2} \cdot a_{l/2} = a_{1/2}$, тобто $b_0 = a_0$, $b_1 = 0$, $b_2 = a_1$, $b_3 = 0$, $b_4 = a_3$,..., $b_{2 \cdot n-2} = a_{n-1}$. Таким чином, поліноміальне представлення квадрату $A \otimes A$ може бути трансформовано до вигляду:

$$P(A \otimes A) = a_{n-1} \cdot x^{2 \cdot n-2} + a_{n-2} \cdot x^{2 \cdot n-4} + ... + a_1 \cdot x^2 + a_0.$$

Ґрунтуючись на властивостях поліноміального квадрату та використані передобчислень може бути реалізовано спосіб прискореного експоненціювання на кінцевих полях. Процедура експоненціювання складається з n циклів послідовного аналізу розрядів експоненти, починаючи зі старшого. Якщо поточний біт експоненти дорівнює одиниці, то виконуються обчислення $R \otimes R \otimes A$ rem M. Якщо $r_0, r_1, ..., r_{n-1}$ - двійкові розряди R, тобто $R = r_0 + r_1 \cdot 2 + r_2 \cdot 2^2 + ... + r_{n-1} \cdot 2^{n-1}$, де $\forall j \in \{0,1,...,n-1\}$ $r_j \in \{0,1\}$, то згідно (2.1) $R \otimes R = r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + ... + r_1 \cdot 2^2 + r_0$. Якщо вважати, що A - множиме, а $P(R \otimes R)$ - множник, то поліноміальний добуток $R|^2 \otimes A$ можна представити у вигляді суми добутків коду А на компоненти квадрату $R|^2$: $R|^2 \otimes A = A \cdot (r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + ... + r_1 \cdot 2^2 + r_0) = A \cdot r_0 \oplus A \cdot 2^2 \cdot r_1 \oplus A \cdot 2^4 \cdot r_2 \oplus ... \oplus A \cdot 2^{2 \cdot n-4} \cdot r_{n-2} \oplus A \cdot 2^{2 \cdot n-2} \cdot r_{n-1})$. Залишок від поліноміального ділення $(R|^2 \otimes A)$ rem M відповідно дорівнює: $(R|^2 \otimes A)$ rem $M = (A \cdot r_0 \oplus A \cdot 2^2 \cdot r_1 \oplus A \cdot 2^4 \cdot r_2 \oplus ... \oplus A \cdot 2^{2 \cdot n-4} \cdot r_{n-2} \oplus A \cdot 2^{2 \cdot n-2} \cdot r_{n-1})$ rem $M = A \cdot r_0 \oplus (A \cdot 2^2)$ rem $M \cdot r_1 \oplus (A \cdot 2^4)$ rem $M \cdot r_2 \oplus ... \oplus (A \cdot 2^{2 \cdot n-4})$ rem M$\cdot r_{n-2} \oplus (A \cdot 2^{2 \cdot n-2})$ rem $M \cdot r_{n-1}$. Очевидно, що значення $A \cdot 2^2$ rem M , $A \cdot 2^4$ rem M, ..., $A \cdot 2^{2 \cdot n-4}$ rem M, $A \cdot 2^{2 \cdot n-2}$ rem M можуть бути обчислені перед експоненціюванням і збережені в таблиці: T[0]=A, T[1]= $A \cdot 2^2$ rem M, T[2]= $A \cdot 2^4$ rem M,..., T[n-2]= $A \cdot 2^{2 \cdot n-4}$ rem M, T[n-1]= $A \cdot 2^{2 \cdot n-2}$ rem M. Відповідно, обчислення організуються згідно з наступного виразу: $(R|^2 \otimes A)$ rem M = T[0]$\cdot r_0 \oplus$ T[1]$\cdot r_1 \oplus$ T[2]$\cdot r_2 \oplus ... \oplus$ T[n-2]$\cdot r_{n-2} \oplus$ T[n-1]$\cdot r_{n-1}$. Аналогічно, якщо поточний біт експоненти дорівнює нулю, то реалізується лише піднесення до квадрату: $R \otimes R$ rem M. У відповідності з (2.1) $R \otimes R = r_{n-1} \cdot 2^{2 \cdot n-2} + r_{n-2} \cdot 2^{2 \cdot n-4} + ... +$

$r_1 \cdot 2^2 + r_0$. Залишок від поліноміального ділення $R|^2$ rem M відповідно в цьому випадку дорівнює: $R|^2$ rem $M = (r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{2 \cdot n-4} \cdot r_{n-2} \oplus 2^{2 \cdot n-2} \cdot r_{n-1})$ rem $M = r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{n-2} \cdot r_{n/2-1} \oplus 2^n$ rem $M \cdot r_{n/2} \oplus ... \oplus 2^{2 \cdot n-2}$ rem $M \cdot r_{n-1}$. Чисельні значення 2^n rem M , 2^{n+2} rem M, ..., $2^{2 \cdot n-4}$ rem M, $2^{2 \cdot n-2}$ rem M можуть бути обчислені перед експоненціюванням і збережені в таблиці W : W[0]= 2^n rem M, W[1]= 2^{n+2} rem M , W[2]=2^{n+4} rem M,..., W[n/2-2]= $2^{2 \cdot n-4}$ rem M, W[n/2-1]= $2^{2 \cdot n-2}$ rem M. З урахуванням наведеного, обчислення $R|^2$ rem M організується в наступному вигляді : $R|^2$ rem M = = $r_0 \oplus 2^2 \cdot r_1 \oplus 2^4 \cdot r_2 \oplus ... \oplus 2^{n-2} \cdot r_{n/2-1} \oplus$ W[0]$\cdot r_{n/2} \oplus$ W[1]$\cdot r_{n/2+1} \oplus ... \oplus$ W[n/2-2]$\cdot r_{n-2} \oplus$ W[n/2-1]$\cdot r_{n-1}$.

Таким чином, для обчислення $A|^E$ rem M на кінцевих полях попередньо виконується формування двох таблиць W та T. Таблиця W не залежить від A, і необхідність її попереднього формування визначається зміною M - числа, що співвідноситься з утворюючим поліномом кінцевого поля. Формування таблиці W виконується у відповідності з алгоритмом: 1. W[0] = 2^n rem M; i = 0; 2. W[i] = 2·W[i-1] rem M, i=i+1; 3. Якщо $i < n/2$, повернення на п.2. Таблиця T заповнюється перед початком обчислення $A|^E$ rem M згідно з наступним алгоритмом: 1. T[0] = A; j = 0; 2. T[j] = 2·T[j-1] rem M, j = j+1; 3. Якщо $j<n$, повернення на п.2.

Процес експоненціювання організовується у вигляді циклу, що повторюється n раз: 1. R=1; j =n-1; 2. Якщо e_j=0 виконання пп. 2.1.-2.5. 2.1. i=0 ; D = 1; S=0; 2.2. Якщо r_i =0, перехід на п. 2.4. 2.3. Якщо $i < n/2$, то S=S+D, інакше S=S+W[i-n/2]. 2.4. D=D ·2; i = i + 1; 2.5. Якщо $i < n$, повернення на п. 2.2., інакше перехід на п. 4. 3. Якщо e_j=1 виконання пп. 3.1.-3.5. 3.1. i=0 ; S=0; 3.2. Якщо r_i =0, перехід на п. 3.4. 3.3. S = S + T[i]; 3.4. i = i + 1 ; 3.5. Якщо $i < n$, повернення на п. 3.2. 4. j = j - 1; якщо $j \geq 0$, то повернення на п. 2

Наведена процедура експоненціювання на скінчених полях Галуа може бути прямо використана для прискореної ідентифікації користувачів.

Реалізована інформаційна технологія включає такі структурні модулі:

1. модуль для знаходження простих поліномів

2. модуль для шифрування повідомлень
3. модуль з реалізацією методу ідентифікації

Проведений аналіз ефективності методу шляхом порівняння часу виконання процедури експоненціювання в різних математичних базисах. Отримані результати свідчать, що швидкість ідентифікації при використанні запропонованого методу зростає на декілька порядків, в порівнянні з відомими методами, що є суттєвим показником

Результати та обговорення./Results and discussion. Запропоновано метод строгої ідентифікації користувачів з використанням незворотних перетворень на полях Галуа, який включає в себе процедуру реєстрації користувача в системі та процедуру одного сеансу ідентифікації. Розроблено метод прискореної строгої ідентифікації користувачів розподілених систем на основі незворотних перетворень алгебри полів Галуа, і який використовує встановлені властивості локальних циклів експоненціювання на полях Галуа, утворюючий поліном яких є добутоком двох простих поліномів.

Висновки./Conclusions. Реалізовано інформаційну технологію ідентифікації користувачів яка ґрунтується на локальних циклах утворюваних при виконанні експоненціювання на полях Галуа на основі методу суворої ідентифікації користувачів з використанням незворотних перетворень на полях Галуа, який включає в себе процедуру реєстрації користувача в системі та процедуру одного сеансу ідентифікації.