УДК 004.052.42

О. Марковський, І. Дайко

МЕТОД КРИПТОГРАФІЧНО СТРОГОЇ ІДЕНТИФІКАЦІЇ НА ОСНОВІ НЕЗВОРОТНИХ ТАБЛИЧНИХ ПЕРЕТВОРЕНЬ НА ПОЛЯХ ГАЛУА

Анотація: Теоретично обґрунтовано, розроблено та досліджено метод ідентифікації учасників віддаленої взаємодії, який забезпечує швидку обчислювальну реалізацію концепції встановлення їх автентичності на основі концепції “нульових знань” з використанням незворотних табличних перетворень на кінцевих полях Галуа GF(2^n). Прискорення криптографічно строгої ідентифікації досягається за рахунок використання для перевірки правильності сеансових паролі експоненціювання на полях Галуа з показником, що являє собою ступінь двійки. Для реалізації цієї операції розроблена таблична технологія, що базується на використання передобчислень і не потребує знання утворюючого поліному поля Галуа.

Детально розроблені процедури, що складають запропонований метод: побудови таблиць передобчислень, авторизації віддаленого абонента, а також його ідентифікації. Виклад ілюстровано прикладом. Теоретично доведено та експериментально підтверджено, що використання запропонованого методу дозволяє прискорити криптографічно строгу ідентифікацію в $12 \cdot n$ раз в порівнянні з відомими.

Ключові слова: ідентифікація на основі концепції нульових знань, криптографічно строга автентифікація, криптографічні алгоритми на основі алгебри полів Галуа, експоненціювання на полях Галу, передобчислення

Вступ

Стимульоване Всесвітньою пандемією COVID-19 динамічне розширення використання віддалених форм інформаційної взаємодії потребує розвитку та вдосконалення відповідної технологічної бази. Значною мірою ефективність віддаленої взаємодії залежить від організації захисту від спроб незаконного отримання даних та прав їх зміни. В більшості випадків такі деструктивні дії відбуваються шляхом спроб підміни учасника дистанційної взаємодії. Тому ключовим елементом захисту виступає надійна ідентифікація її учасників.

Розширення сфер застосування дистанційних форм інформаційної взаємодії значною мірою відбувається за рахунок тих із них, які потребують підвищеної надійності ідентифікації її учасників. Це, в першу чергу, стосується сфер фінансової та банківської діяльності, комерційного надання послуг, віддаленого адміністрування діяльності та управління об’єктами реального світу.

З іншого боку, збільшення учасників інформаційної взаємодії, а також зростання питомої ваги систем, що працюють в режимі реального часу диктує необхідність прискорення комп’ютерної реалізації процедур ідентифікації.

Вирішення цих, продиктованих реаліями сьогодення вимог до перспективних засобів ідентифікації віддаленої взаємодії потребує пошуку принципового нових підходів та рішень.

Таким чином, наукова задача підвищення ефективності методі та засобів ідентифікації учасників віддаленої інформаційної взаємодії є актуальною та практично вагомою виходячи з реалій сучасного етапу розвитку інформаційних технологій.

Огляд сучасних методів криптографічно строгої ідентифікації

Задача ідентифікації віддалених учасників інформаційної взаємодії займає чільне місце в сучасній криптографії. Існує декілька теоретичних моделей задачі ідентифікації [1]. Зазвичай, розглядається модель ідентифікації великої кількості абонентів певної системи колективного доступу, яка надає користувачам певні ресурси на комерційній основі [2].

Ідентифікація в рамках цієї моделі полягає в наданні віддаленим користувачем певної інформації системі в формі паролю. Відповідно, ціль зловмисника полягає в підробці паролю з метою незаконного отримання від системи певних ресурсів. Для цього зловмисник може використовувати такі можливості:

- перехопити пароль на етапі його вводу або передачі в систему з тим, щоб повторно використати для незаконного входу;

- отримати пароль шляхом проникнення в систему і, зокрема, отримання доступу до пам'яті паролів через використання вірусів, спеціальних атак під виглядом легального користувача.

Окремий вид атак на віддалену взаємодію полягає в перехопленні процесу обміну даних після ідентифікації з витісненням легального абонента (middle atttacks) .

 ISSN 1560-8956

В зв’язку з динамічною комерціалізацією дистанційного надання різноманітних послуг з'явився новий вид зловживань: імітація надання платних послуг з боку системи [2].

В теоретичному плані методи ідентифікації розділяються на два класи: криптографічно строгі та слабкі [2]. До класу криптографічно слабких відносяться схеми ідентифікації, в яких пароль абонента залишається незмінним із сеансів взаємодії і він відомий системі [2]. Зрозуміло, що пароль може бути перехоплено зловмисником або отримано в разу доступу до пам'яті системи. Для запобіганню останнього в багатьох схемах криптографічно слабкої ідентифікації пароль зберігається в пам'яті системи у вигляді його хеш-сигнатури.

Більшість існуючих методів криптографічно строгої ідентифікації віддалених абонентів базуються на теоретичній концепції “нульових знань” (zero knowledge identification). Ця концепція передбачає виконання наступних умов:

- абонент має спеціальний математичний механізм генерації правильних паролів, які змінюються в кожному сеансі дистанційної взаємодії;

- система має в своєму розпорядженні математичний механізм перевірки правильності паролю конкретного абоненту, при цьому система сама не здатна формувати правильні паролі.

До теперішнього часу запропонована доволі значна кількість схем ідентифікації, які реалізують теоретичну концепцію “нульових знань”. Їх порівняльна оцінка може бути здійсненна виходячи з таких критеріїв ефективності:

- рівнем захищеності, який оцінюється об’ємом ресурсів, які потрібно витратити зловмиснику або системі для підробки правильного паролю;

- часом обчислювальної реалізації процедури криптографічно строгої ідентифікації, тобто механізму перевірки системою правильності надісланого їй паролю.

Всі існуючі схеми криптографічно строгої ідентифікації можна поділити на два класи:

- схеми ланцюжкової ідентифікації, в яких сеансові паролі функціонально пов’язані між собою;

- схеми ідентифікації з функціонально непов’язаними між собою сеансовими паролями.

Схеми ланцюжкової ідентифікації використовують послідовність

сеансових паролів $P_1,P_2,\ldots,P_m$ пов’язаних між незворотними математичними перетвореннями φ: $P_1 = \varphi(P_2)$, $P_2 = \varphi(P_3),\ldots,P_{n-1} = \varphi(P_n)$. На етапі авторизації абонент повідомляє системі код P_1. В якості паролю в першому сеансі абонент використовує P_2. Відповідно, система виконує над отриманим паролем незворотне перетворення $\varphi(P_2)$ і порівнює отриманий результат з кодом P_1: $\varphi(P_2)=P_1$, то ідентифікація абонента вражається успішною і код P_2 в пам'яті системи заміщає P_1. Аналогічним чином здійснюється ідентифікація на інших (n-2)-х сеансах. В якості незворотного перетворення використовуються стандартизовані хеш-перетворення [3] або шифроблоки [4], які швидко реалізуються програмно або з застосуванням криптопроцесорів. Основна перевага використання ланцюжкової ідентифікації полягає в високій швидкості. Недоліками таких схем є обмежена кількість сеансів взаємодії та можливість втрати синхронізації використання паролів абонентом та системою.

Схеми криптографічно строгої ідентифікації з функціонально непов’язаними між собою сеансовими паролями мають за основу використання різних незворотних перетворень. Найбільш часто в якості останніх застосовуються незворотні перетворення теорії чисел. Типовою схемою такого типу, яка реалізує ідентифікацію в рамках концепції нульових знань є FFSIS (Feige Fiat Shamir Identification Scheme) [5]. Основний недолік цієї схеми полягає в низькій швидкодії, зумовленій багатократним виконанням операції модулярного множення над числами великої розрядності.

Інші, широко відомі схеми криптографічно строгої ідентифікації на основі важкорозв'язних задач теорії чисел, такі як схема Guillou-Quisquater [6] та Schnorr [7] використовують операцію модулярного експоненціювання $A^E \bmod M$. Обчислення модулярної експоненти n–розрядних чисел на r-розрядному процесорі потребує $6\cdot n^3/r$ процесорних операцій.. Беручи до уваги, що в практичних застосуваннях n=2048 або n=4096, ясно, що реалізація ідентифікації за вказаними методами потребує значних часових ресурсів.

Для прискорення криптографічно строгої ідентифікації запропоновані методи, в яких експоненціювання реалізується в алгебрі кінцевих полів Галуа [8]. Використання цієї алгебри дозволяє суттєвим чином спростити обчислення, проте в відомих схемах для експоненціювання використовуються класичні алгоритми, які потребують складних операцій редукції на полі Галуа, що обмежує швидкодію цих методів.

Таким чином, аналіз відомих методів криптографічно строгої ідентифікації показав, що найбільш функціонально досконалі методи, для яких відсутні обмеження на кількість сеансів дистанційної взаємодії базуються на складних в обчислювальному плані операціях, що зумовлює їх недостатню, з позицій сучасних вимог, швидкодію.

Мета досліджень полягає в підвищенні ефективності криптографічно строгої ідентифікації віддалених абонентів за рахунок прискорення її обчислювальної реалізації.

Організація табличного піднесення до степені 2^k на полях Галуа

Кінцеві поля Галуа широко використовуються в сучасних механізмах криптографічного захисту інформації. Зокрема, вони лежать в основі побудови генераторів псевдовипадкових двійкових послідовностей, стандарту симетричного шифрування AES, використовуються в еліптичній криптографії [9], реалізації ідентифікації в рамках прогресивної концепції нульових знань [8], а також для побудови криптографічних механізмів з відкритим ключем [10].

Базовою обчислювальною операцією багатьох з цих застосувань є експоненціювання на кінцевих полях Галуа GF(2^n). На відміну від традиційної алгебри при використанні полів Галуа обчислення арифметичної суми замінюється на логічне додавання (XOR), яке позначається символом ’⊕’, замість арифметичного множення використовується поліноміальне множення (множення без переносів), яке позначається символом ’⊗’ [8]. В силу того, що при поліноміальному множенні і, відповідно, при піднесенні до степені ступінь поліному $Y(x)$ результату значно перевищує ступінь n утворюючого поліному $P(x)$ поля Галуа, над результатом здійснюється операція редукції, тобто віднаходження залишку від поліноміального ділення $Y(x)$ на утворюючий поліном поля, яка позначається як Y(x) rem $P(x)$ або Y rem P [8].

Число A, над яким здійснюється операція піднесення до степені 2^k на кінцевому полі Галуа що породжене простим поліномом $P(x) = x^n + p_{n-1}\cdot x^{n-1}+\ldots+p_2\cdot x^2 + p_1\cdot x + p_0$ може бути представлене у вигляді полінома ступеня n-1: $A(x) = a_{n-1}\cdot x^{n-1} + a_{n-2}\cdot x^{n-2}+\ldots+a_1\cdot x + a_0$, $\forall j\in\{0,1,..,n\text{-}1\}$: $p_j,a_j\in\{0,1\}$. Відповідно, квадрат числа A може бути представлений у вигляді наступної формули:

$$A^2 \, rem \; P = \bigoplus_{i=0}^{n-1} \bigoplus_{l=0}^{n-1} a_i \cdot a_l \cdot x^{i+l} \; rem \; P \, . \qquad (1)$$

В силу того, що за умови $i \neq l$ логічна сума симетричних компонентів дорівнює нулю, тобто $a_i \cdot a_l \cdot x^{i+l} \oplus a_l \cdot a_i \, x^{l+i} = 0$, формула (1) може бути приведена до вигляду:

$$A^2 \; rem \; P = \bigoplus_{l=0}^{n-1} (a_l \cdot x^{2 \cdot l} \, rem \; P) \; . \tag{2}$$

Аналіз формули (2) дозволяє зробити висновки про те, що квадрат на полі Галуа може бути обчислений у вигляді логічної суми результатів редукції вагових коефіцієнтів парних ступенів, помножених на відповідні біти двійкового представлення числа A.

Аналогічними перетвореннями формула для обчислення числа A в четвертій степені на полі Галуа може бути представлена наступним чином:

$$A^4 \; rem \; P = \bigoplus_{l=0}^{n-1} (a_l \cdot x^{4 \cdot l} \, rem \; P) \; . \tag{3}$$

В узагальненому виді формула для обчислення експоненти числа A з показником 2^k на полі Галуа, утвореного простим поліномом $P(x)$ має наступний вигляд:

$$A^{2^k} \; rem \; P = \bigoplus_{l=1}^{n-1} (a_l \cdot x^{2^k \cdot l} \; rem \; P) \, . \tag{4}$$

З формули (4) випливає, що найбільш ресурсоємка частина обчислення, а саме віднаходження залишків від ділення $x^{2^k}, x^{2 \cdot 2^k}, ..., x^{(n-1) \cdot 2^k}$ на утворюючий поліном $P(x)$ не залежить від числа А над яким здійснюється експоненціювання, а значить, може бути реалізована в формі передобчислень, які виконуються лише один раз. Для збереження і застосування результатів таких передобчислень пропонується використання таблиці, яка містить n значень: T[0], T[1] ,…, T[n-1], що обчислюються за формулою:

$$\forall l \in \{0,1,..., n-1\} : T[l] = 2^{l \cdot 2^k} \; rem \; P \, . \tag{5}$$

Відповідно, при використанні таблиць передобчислень, формула для обчислення експоненти числа A з показником 2^k на полі Галуа, утвореного простим поліномом $P(x)$ трансформується до наступного виду:

$$A^{2^k} \; rem \; P = \bigoplus_{l=1}^{n-1} a_l \cdot T[\, l \,] \, . \tag{6}$$

Наприклад, якщо n=8, а в якості утворюючого поліному поля Галуа GF(2^8) обрано простий поліном $P(x) = x^8 + x^6 + x^5 + x + 1$, який спів носиться з числом P =

 ISSN 1560-8956

101100101_2 = 357. Для цього поліному при k=1 таблиця передобчислень має вигляд представлена у вигляді табл. 1.

Таблиця 1. **Приклад таблиці передобчислень для** $P(x) = x^8 + x^6 + x^5 + x + 1$

l	**T [*l*]**	***l***	**T [*l*]**
0	1	4	101
1	4	5	241
2	16	6	107
3	64	7	201

При піднесенні до квадрату, тобто при k=1 в ступінь 2^1 числа A=115 = 1110011_2 організується цикл проходу двійкових розрядів числа A. Якщо і-тий, $i \in \{0,1,\ldots,n-1\}$, розряд a_i числа A дорівнює одиниці, тобто a_i=1, то до результату R логічно додається відповідне значення T[i] таблиці передобчислень. Для поточного прикладу результат обчислюється у вигляді наступної логічної суми: R = T[0] ⊕ T[1] ⊕ T[4] ⊕ T[5] ⊕ T[6] = 1 ⊕ 4 ⊕ 101 ⊕ 241 ⊕ 107 = 250. Легко перевірити, що (115⊗115) rem 357 =250.

Таким чином, запропонований метод піднесення числа A на полі Галуа в ступінь 2^k з застосуванням таблиці передобчислень дозволяє виконати ці обчислення без використання утворюючого поліному P(x). При цьому середній час T_T експоненціювання не залежить від значення k і становить $T_T = 0.5 \cdot n \cdot t_{xor}$, де t_{xor} – час логічного додавання n-розрядних чисел.

Метод криптографічно строгої ідентифікації на основі табличної реалізації незворотних перетворень на полях Галуа

Викладена вище технологія піднесення до степені 2^k на полях Галуа на основі таблиць передобчислень покладена в основу запропонованого методу криптографічно строгої ідентифікації. Фактично для піднесення будь-якого числа в ступінь 2^k на полях Галуа з використанням таблиць передобчислень не потрібно знати утворюючий поліном поля. Це означає, що системі на етапі авторизації користувача може бути повідомлена лише обчислена ним таблиця передобчислень. Тоді система в змозі реалізувати експоненціювання на полях Галуа з показником, що може бути представленим у вигляді лінійної комбінації 2^k. Іншими словами, система здатна обчислювати експоненту A^G rem P на кінцевому полі Галуа не маючи у своєму розпорядженні утворюючого поліному $P(x)$, за умови, що $G=\lambda \cdot 2^k$, де λ-ціле число.

$$G = \sum_{i=1}^{\frac{1}{k}\cdot\log_2 n} \lambda_i \cdot 2^{i\cdot k}, \forall i \in \{1,2,..., \frac{\log_2 n}{k}\} : \lambda_i \in \{0,1\}. \quad (7)$$

Для інших значень показника ступеню G, відмінних від (7) система не в змозі обчислити експоненту на полі Галуа.

На відміну від модулярної арифметики, довжина циклу *L* експоненціювання на полях Галуа, за умови що якості утворюючого поліному використовуються прості поліноми, залежить не від виду утворюючого поліному, а тільки від його ступеню [7]. Зокрема, якщо поле Галуа GF(2^n) утворене простим поліномом *P*(*x*) ступеня *n*, то довжина циклу експоненціювання становить: $L= 2^n$ [7]. Це означає, що для будь-якого поліному *A*(*x*) ступеня *n*-1 виконується рівність:

$$A(x)^{2^n} \; rem \; P(x) = A(x). \quad (8)$$

Ідея, покладена в основу запропонованого методу ідентифікації, що реалізує концепцію ”нульових знань”, полягає в тому, що перевірка правильності пред’явленого абонентом сеансового паролю здійснюється шляхом його піднесення на полі Галуа до ступеня $h=2^k$. При цьому результат цієї операції порівнюється зі сформованим самою системою кодом доступу Y. Тобто, в якості сеансового паролю виступає $U=Y^w$ rem *P*, яке принципового не може бути обчислене системою. Обчислення *U* може здійснити лише абонент, який володіє секретним елементом - кодом утворюючого поліному *P*(*x*) поля Галуа.

Очевидно, що для того, щоб виконувалася умова прийняття рішення про успішність ідентифікації: U^h rem $P = Y$ має виконуватися наступна умова:

$$\gamma \cdot (2^n - 1) + 1 = 2^k \cdot w, \quad (9)$$

де γ - ціле число. Зрозуміло, що для того, щоб система не могла обчислити самостійно значення сеансового паролю *U*, для ступеня *w* не має виконуватися умова (9), тобто *w* не може бути представлене у вигляді лінійної комбінації ступенів 2^k. Іншими словами, значення γ має бути обрано абонентом таким чином, щоб одночасно виконувалися дві умови:

$$\begin{aligned} &(\gamma \cdot (2^n - 1) + 1) \bmod 2^k = 0, \\ &((\gamma \cdot (2^n - 1) + 1) \cdot 2^{-k}) \bmod 2^k = 1 \end{aligned}. \quad (10)$$

Наприклад, якщо *n*=8 і *k*=1, то умова (10) виконується для γ=3, для γ=7 і для γ=11. Після вибору числа γ, яке не є секретним, абонент обчислює значення

 ISSN 1560-8956

w за наступною формулою:

$$w = \frac{\gamma \cdot (2^n - 1) + 1}{2^k}. \qquad (11)$$

В рамках прикладу, що розглядається, при γ=3 обчислене за формулою (11) значення w дорівнює w=383. Цілком очевидно, що згідно першої умови (10) значення w – ціле числа, а у відповідністю з другою умовою (10) число w не ділиться на 2^k, тобто його не можна представити і формі (7). В практичному плані це означає, що система, не маючи в своєму розпорядженні обраного абонентом утворюючого поліному $P(x)$ принципово не здатна піднести на цьому полі Галуа будь-яке число в ступінь w.

Таким чином, на етапі авторизації, згідно запропонованого методу, віддалений абонент виконує наступну послідовність дій:

1. Обирає довільним чином один із простих поліномів $P(x)$ ступеня n.

2. Обирає довільним чином значення k.

3. Обирає одне зі значень цілого числа γ, яке задовольняє умовам (10)

5. Обчислює значення ступеня w за формулою (11).

6. Формує з використанням формули (5) таблицю передобчислень.

7. Довільним чином обирає ключ ϑ формування розширення коду доступу.

8. З використанням відкритого ключа K_P системи обраний ключ ϑ та таблиця T передобчислень шифруються і надсилаються системі.

9. Система з використанням свого секретного ключа K_C дешифрує надіслану інформацію і зберігає ключ ϑ та таблицю передобчислень користувача.

Процедура ідентифікації віддаленого користувача на початку сеансу його дистанційної взаємодії з системою передбачає виконання наступний дій:

1. Користувач довільним чином формує $0.5 \cdot n$-розрядний код доступу X і надсилає його системі.

2. Система отримує код доступу X і обчислює його $0.5 \cdot n$-розрядне розширення E як результат шифрування добу доступу з застосуванням ключа ϑ: $E = C(X, \vartheta)$, де C – функція шифрування. Код Y формується як конкатенація коду доступу X та обчисленого його розширення E: Y=X|E.

3. Сформований системою код Y надсилається користувачеві. .

4. Користувач обчислює код E' розширення коду доступу X шляхом

шифрування його секретним ключем ϑ: $E' = C(X,\vartheta)$, після чого порівнює отриманий код E' з молодшими n/2 розрядами коду Y, упевнюючись в тому, що код Y надісланий йому саме системою, яка знає секретний ключ ϑ.

5. Користувач обчислює $U=Y^w \text{ rem } P$ за відомими алгоритмами експоненціювання на полях Галуа.

6. Обчислений код U в якості сеансового паролю користувач надсилає системі.

7. Система приймає код U сеансового паролю користувача і обчислює $Y' = U^{2^k} rem\ P$ за формулою (6) з використанням таблиць передобчислень.

8. Система порівнює сформований нею код Y та обчислений Y′ за отриманим сеансовим паролем U. Якщо ці коди співпадають, тобто Y = Y′, то ідентифікація віддаленого користувача вважається успішною.

В якості функції C (X,ϑ) шифрування може бути використано будь-який алгоритм симетричного шифрування (наприклад DES, AES).

Робота наведеної процедури ідентифікації віддаленого користувача перед початком його дистанційної взаємодії з системою ілюструється наступним прикладом. Нехай, n=8 і на етапі авторизації користувач обрав в якості утворюючого для поля Галуа простий поліном $P(x) = x^8 + x^6 + x^5 + x + 1$, який співноситься з числом $P = 101100101_2 = 357$. Користувачем також обрано значення k=1 і за формулою (кК) обчислено значення w=383. Крім цього користувач сформував таблицю передобчислень для піднесення числа до квадрату на обраному полі Галуа, яка наведена в табл. 1. Нарешті, користувач обрав ключ $\vartheta = 14 = 1100_2$ для утворення розширення коду доступу. Вказаний код $\vartheta = 14$ разом з таблицею передобчислень користувач шифрує відкритим ключем системи і надсилає їй. Система з використанням свого секретного ключа розшифровує надіслані дані і зберігає код ϑ та таблицю передобчислень в пам'яті.

На початку сеансу дистанційної взаємодії з системою користувач генерує 4-розрядний код $X = 1001_2 = 9$ і надсилає його системі. Остання, у відповідності з п.2 формує його 4-розрядне розширення $E = C(X,\vartheta) = C(9,14)$. Якщо припустити, що результат шифрування $E = C(X,\vartheta) = C(9,14) = 13 = 1101_2$, то код Y формується як конкатенація : $Y=X|E = 10011101_2 = 157$. Вказаний код Y= 157 повертається користувачеві. Той переконується, що молодші чотири розряди отриманого коду співпадають з результатом шифрування старших 4-х розрядів

 ISSN 1560-8956

ключем ϑ=14. Це означає, що код Y надісланий йому системою, яка знає секретний ключ ϑ.

З застосуванням одного із класичних алгоритмів експоненціювання на полях Галуа користувач обчислює експоненту отриманого коду Y= 157 в степені w=383: $U = 157^{383}$ rem 357 = 142. Отриманий код U=142 використовується користувачем в якості сеансового паролю і надсилається в систему. Система підносить отриманий код до квадрату на полях Галуа з використанням таблиць передобчислень. Двійковий код $142 = 10001110_2$. Відповідно Y′ обчислюється у вигляді логічної суми табличних значень номерів одиничних розрядів : Y′= T[1] ⊕ T[2] ⊕ T[3] ⊕ T[7] = 4 ⊕ 16 ⊕ 64 ⊕ 201 = 157. Система порівнює обчислений код Y′=157 з раніше сформованим кодом Y=157. Оскільки вони співпадають, приймається рішення на користь успішної ідентифікації користувача, якому надаються відповідні права доступу до ресурсів системи.

Запропонований спосіб являє собою технологію криптографічно строгої ідентифікації с силу того, що він задовольняє вимогам теоретичної концепції “нульових знань”. Користувач має в своєму розпорядженні математичний апарат формування правильних сеансових паролі. Роль вказано механізму відіграє класичний алгоритм піднесення числа в довільну ступінь на полях Галуа. Секретним елементом цього механізму виступає обраний користувачем утворюючий поліном поля. Це означає, що лише користувач може підносити числа в будь-яку ступінь на обраному користувачем кінцевому полі Галуа.

В розпорядженні системи є механізм перевірки правильності сеансового паролю у вигляді таблиць передобчислень, яка дозволяє системі без знання утворюючого поліному поля Галуа підносити числа на цьому полі в ступінь 2^k. Оскільки вказаний механізм не дозволяє підносити числа на конкретному полі Галуа в іншу ступінь, система самостійно не здатна генерувати правильні сеансові паролі.

З викладено вище цілком ясно, що запропонований метод не накладає реальних обмежень на кількість сеансових паролів які можуть використовуватися.

Оцінка ефективності

Порівняльну оцінку ефективності запропонованого методу криптографічно строгої ідентифікації віддалених учасників інформаційної взаємодії доцільно здійснити за двома базовими критеріями:

- рівнем захищеності, тобто визначення об’єму ресурсів, потрібних для порушення захисту:

- часовими характеристиками здійснення криптографічно строгої ідентифікації.

Рівень захищеності може бути визначено об’ємом потрібних для цього ресурсів с позицій стороннього зловмисника та з позицій самої системи, яка може мати інтерес комерційного плану для фальшування правильних паролів. Зрозуміло, що система має доступ до суттєво більшого об’єму інформації в порівнянні зі стороннім зловмисником. Відповідно, якщо провести оцінку захищеності з позицій фальшування паролю користувача з боку системи, то ясно, що стороннього зловмисника рівень захищеності є значно вищим.

Система може випадковим чином обрати код U сеансового паролю, маючи в наявності таблиці передобчислень отримати значення $Y = U^{2^k} rem\ P$ і вважати, що саме отриманий код Y був сформований системою. Проте, молодші $n/2$ розрядів Y – що утворюють код E, мають функціонально залежати від старших $n/2$ бітів Y, які утворюють код X: $E = C(X,\vartheta)$. Тому тактика випадкового підбору коду U сеансового паролю системою має ймовірність успішності, яка дорівнює $2^{-n/2}$. При n=1024 чисельне значення ймовірності того, що така спроба виявиться успішною становить $2^{-512} \approx 10^{-154}$. Ясно, що підбір паролю таким способом потребує ресурсів, що далеко перевищують можливості практичної реалізації.

Інша тактика системи по фальшуванню правильного сеансового паролю користувача полягає в підборі утворюючого поліному $P(x)$ поля Галуа, яке використовується при ідентифікації. Верхня границя кількості простих поліномів n-го ступеня для полі Галуа $GF(2^n)$ дорівнює $(2^n-1)/n$ [9]. Тобто для n=1024 існує близько $1.7 \cdot 10^{308}$ простих поліномів, перебір яких практично виключається з огляду на потрібний для цього об’єм обчислювальних ресурсів.

Таким чином, показано, що система, яка володіє суттєво більшою інформацією в порівнянні зі стороннім зловмисником, практично не здатна підробити правильний пароль віддаленого користувача.

При оцінюванні часової ефективності запропонованого методу слід взяти до уваги специфіку дистанційної взаємодії. Якщо розглядати інтегровані системи надання ресурсів великій кількості віддалених користувачів, то критичним параметром слід вважати час ідентифікації системою. Дійсно, якщо

система обслуговує сотні тисяч віддалених користувачів, то критично важливим є час, який витрачається системою для ідентифікації окремого користувача. При цьому час, який витрачає користувач на виконання процедури ідентифікації не є критичним. В запропонованому методі користувач має змогу заздалегідь згенерувати випадковий код числа X, сформувати його розширення E, отримати код Y конкатенацією X і E, а також обчислити сеансовий пароль $U=Y^w \text{ rem } P$. Тобто час виконання переважної частини ідентифікації користувачем не впливає на критичні часові характеристики запропонованого методу.

Реально швидкість ідентифікації визначається часом піднесення на полі Галуа системою отриманого від користувача сеансового паролю в ступінь 2^k з використанням таблиці передобчислень. Як було показано вище, середній час T_T експоненціювання не залежить від значення k і становить $T_T = 0.5 \cdot n \cdot t_{xor}$, де t_{xor} – час логічного додавання n-розрядних чисел. При реалізації на r-розрядному процесорі $t_{xor} = n \cdot \tau / r$, де τ-час виконання процесорної операції. Відповідно: $T_T = 0.5 \cdot n^2 \cdot \tau / r$. Еспоненціювання на полях Галуа за відомими технологіями з використанням модифікованої редукції Монтгомері потребує часу $T_0 = 6 \cdot n^3 \cdot \tau / r$ [10]. Таким чином, коефіцієнт β прискорення ідентифікації віддалених абонентів, яке досягається застосуванням запропонованого методу в порівнянні з відомими визначається наступним чином:

$$\beta = \frac{T_0}{T_T} = \frac{6 \cdot \frac{n^3}{r} \cdot \tau}{0.5 \cdot \frac{n^2}{r} \cdot \tau} = 12 \cdot n \,. \qquad (12)$$

Таким чином, застосування запропонованого методу за рахунок табличної реалізації операції експоненціювання на полях Галуа з показником, що є ступеню двійки, дозволяє прискорити процес ідентифікації віддалених абонентів в $12 \cdot n$ раз в порівнянні з відомими схеми криптографічно строгої ідентифікації.

Проведені експериментальні дослідження, в цілому підтвердили отриману теоретичним шляхом оцінку прискорення.

Висновки

В результаті проведених досліджень, направлених на підвищення ефективності захисту від стороннього втручання віддаленої інформаційної взаємодії системи та абонентів запропоновано метод криптографічно строгої їх

ідентифікації на основі незворотних операцій на кінцевих полях Галуа.

Розроблений метод криптографічно строгої ідентифікації відрізняється тим, що сторона, яка здійснює ідентифікацію, не маючи доступу до утворюючого поліному поля Галуа, може лише перевіряти правильність надісланого їй сеансового паролю шляхом табличної реалізації операції його експоненціювання на полях Галуа з показником, що є ступеню двійки, за рахунок чого досягається прискорення обчислювальної реалізації процесу встановлення автентичності учасника дистанційної взаємодіїю.

Метод базується на властивостях експоненти на полях Галуа з показником, що є ступеню двійки, а також на використанні передобчислень, які залежать тільки від утворюючого поліному поля. Показано, що запропонований метод реалізує теоретичну концепцію “нульових знань”, тобто надає абоненту математичний апарат генерації коректних сеансових паролів, а системі – математичний механізм перевірки їх коректності.

Теоретично доведено і експериментально підтверджено, що використання запропонованого методу дозволяє за рахунок табличних обчислень на 2-3 порядки прискорити процес криптографічно строгої ідентифікації віддалених абонентів в порівнянні з відомими методами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Schneier B.* Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed.John Wiley, 1996 - 758 p.

2. *Mu Han* Zero-knowledge identity authentication for internet of vehicles: Improvement and application. / Mu Han, Yin Zhikun, Chen Pengzhou, Zhang Xing, Ma Shidian.// PLoS ONE.- 2020.- Vol.15 –No.9.-P.217-247. DOI.ORG/10.137/journal.pone.0239043

3.*Lamport L.* Password Authentication with Insecure Communication / L.Lamport //Communications of the ACM. -1981.- Vol.24.- № 11,- P.770-772.

4. *Bardis N.* Zero-Knowledge Identification Method Based on Block Ciphers / N. Bardis, N. Doucas, O. Markovskyi // Proceeding of 2017 International Conference on Control, Artificial Intelligence, Robotic & Optimization (ICCAIRO). May 2017. DOI: 10.1109/ICCARO.2017.63.

5. *Feige U.* Zero knowledge proofs of identity / U.Feige, A. Fiat, A.Shamir A.// Journal of Cryptology, - 1988.- Vol.1.- №.2. – P.77-94.

6. *Schnorr C.P.* Method for Identification Subscribers and for Generating and Verificating Electronic Signatures in data Exchange System. - US Patent #4995,083.19- 1991.

7. *Guillou L.C.* A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memore / L.C. Guillou, J.J. Quisquater // Proceeding of Advances of Cryptology – Eurocrypt-88.- Springer-Verlag.- 1988.- P.123-128.

8. *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 // Электронне моделювання. 2017.- № 6.- С.96-110.

9. *Николайчук Я.М.* Коди полів Галуа: теорія і застосування / Я.М. Николйчук //Тернопіль.-Вид-во ТНУ. —2012. - 576 с.

10. *Калмиков І.А*. Розробка методу нелінійного шифрування інформації з використанням операції піднесення до степеня для кінцевого поля Галуа / І.А. Калмиков, Е.С. Степанова, К.Т. Тинчеров// Сучасні наукомісткі технології. - 2019.- № 9. - С.84—89.