УДК 004.052.42 DOI: 10.18372/2073-4751.85.21096

Марковський О. П.,
orcid.org/0000-0003-3484-4233,
markovskyy@i.ua,
Дайко І. В.,
orcid.org/0000-0002-5316-7080,
igordaiko1604@gmail.com,
Григораш Ю. В.,
orcid.org/0009-0000-3863-2298,
gyv220427@gmail.com

ПІДХІД ДО РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНОЇ КОНЦЕПЦІЇ НУЛЬОВИХ ЗНАНЬ ДЛЯ ПРИСКОРЕНОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ

НТУУ "Київський політехнічний інститут ім. Ігоря Сікорського"

Вступ

В останні десятиліття прискореними темпами розвиваються технології віддаленої інформаційної взаємодії, а також інтенсивно розширюються сфери їх застосування. . Одним з чинників, що підштовхнув до розкриття потенціалу цих технологій стала пандемія Covid-19. З її закінченням, технічний прогрес Інтернету симулює подальше інтенсивне розширення сфер використання технологій віддаленої інформаційної взаємодії. Для значної частини нових сфер застосування цих технологій принципового важливим є забезпечення високого рівня захищеності та надійного розмежування прав доступу до управління та ресурсів. Мова йде, насамперед, про такі сфери, як дистанційна медицина, банківська справа, віддалене управління та адміністрування. Невпинний процес комерціалізації віддаленого надання різноманітних інформаційних послуг також потребує високого рівня захищеності.

Наріжним каменем в забезпеченні безпеки дистанційної інформаційної взаємодії виступає ідентифікація її учасників. В теоретичному плані спроби отримання доступу до паролю легального учасника дистанційної інформаційної взаємодії можуть здійснюватися як на рівні каналу обміну даними, так і на рівні іншого учасника взаємодії [1]. Теоретично, найбільший захист від спроб незаконного відтворення паролю регального учасника на обох зазначених рівнях забезпечує ідентифікація, що базується на криптографічній концепції "нульових знань" [2]. Тому в останні роки відмічається [3] невпинне зростання питомої ваги саме цієї технології ідентифікації учасників дистанційної інформаційної взаємодії. Основний чинник, що стримує широке використання цього найбільш захищеного виду ідентифікації полягає в тому, що її реалізація потребує значних часових ресурсів [4]. Особливо це критично для інтегрованих систем колективного доступу, що дистанційно взаємодіють з тисячами віддалених абонентів.

Для розширення практичного використання прогресивних технологій ідентифікації абонентів на основі концепції "нульових знань" в таких системах постає задача пошуку можливостей радикального прискорення комп'ютерної реалізації відповідних механізмів ідентифікації насамперед, на стороні системи, як більш навантаженої сторони дистанційної інформаційної взаємодії.

Таким чином, наукова задача прискорення комп'ютерної реалізації ідентифікації на основі теоретичної концепції "нульових знань" є актуальною та практично значимою для сучасного етапу розвитку інформаційних технологій.

Огляд відомих методів ідентифікації на основі концепції "нульових знань"

Як зазначалося вище, з теоретичної точки зору найвищий рівень захищеності від підробки паролю абоненту забезпечується при використанні криптографічної концепції "нульових знань" [5]. Сутність вказаної концепції полягає в тому, що абонент на кожному сеансі віддаленої взаємодії з системою використовує інший сеансовий пароль, що робить неефективним його перехоплення. Кожен із сеансових паролів має певні властивості, які визначають його коректність [6]. Відповідно, абонент володіє секретним криптографічним механізмом формування коректних паролів, а система має у своєму розпорядженні механізм перевірки коректності паролю. Разом з тим, наявність цього механізму не дозволяє системі самостійно генерувати коректні паролі абонента.

Значна частина існуючих методів ідентифікації, що реалізують вказану концепцію "нульових знань" базується на незворотних перетвореннях теорії чисел. Зокрема метод Guillou-Quisquater [7] використовує незворотні перетворення, аналогічні широко відомому алгоритму RSA [2]. На етапі авторизації абонент формує два числа U та W, такі, що $W \cdot D^U \bmod M = 1$. Модуль M, а також сформовані числа U та W передаються системі в якості відкритого ключа абонента.

При ідентифікації абонента, ним генерується випадкове число X та обчислюється перша компонента коректного сеансового паролю $P_1 = X^U \bmod M$. Система випадковим чином генерує $S<U$ і надсилає це число абоненту. Останній формує другу компоненту коректного сеансового паролю $P_2 = X \cdot D^S \bmod M$. Після отримання від абонента обох компонент коректного сеансового паролю система обчислює $R = P_2^U \cdot W^S \bmod M$, якщо $R=P_1$ то ідентифікація вважається успішною.

Основний недолік розглянутого методу полягає в значному обсягу обчислень, що здійснюються системою для перевірки коректності двокомпонентного паролю. Фактично, для перевірки потрібно здійснити дві операції модулярного експоненціювання над числами великої розрядності. При цьому обсяг обчислень може бути оцінено в $6 \cdot n^3/r$ процесорних операцій [8] , де n і r – розрядності чисел та процесора, відповідно·

Ще один метод ідентифікації на основі криптографічної концепції нульових знань запропоновано Schnorr C.P. [9]. Метод також використовує для побудові механізму генерації сеансових паролів незворотні перетворення теорії чисел. Для перевірки системою коректності сеансового паролю також використовуються дві операції модулярного експоненціювання, що здійснюються над довгими числами. Тобто, за часовими характеристиками, метод близький до розглянутого вище методу Guillou-Quisquater. В роботі [10] запропоновано прискорену версію методу Schnorr з блокуванням повторного використання сеансових паролів.. Прискорення досягнуте за рахунок застосування передобчислень при реалізації операцій модулярного експоненціювання.

Для підвищення швидкодії ідентифікації на основі криптографічної концепції нульових знань може бути ефективно застосовано перехід в алгебру скінчених полів Галуа $GF(2^n)$ [11]. Це зумовлене тим, що операції експоненціювання на полях Галуа, в силу специфічних властивостей останніх [12], здійснюють значно простіше і швидше.

Реальне прискорення процедур ідентифікації на основі концепції “нульових знань” при використанні незворотних перетворень на скінчених полях Галуа становить 1-2 порядки [12]. Проте, архітектура сучасних процесорних засобів не пристосовані для виконання операцій на кінцевих полів Галуа. Крім того, застосування алгебри полів Галуа виключає можливість застосування існуючих на сьогоднішній день засобів апаратного прискорення операції модулярного експоненціювання довгих чисел.

Ще один напрямок прискорення ідентифікації, що базується на принципах “нульових знань” полягає в використанні альтернативних незворотних задач криптографії. Зокрема, в сучасній криптографії широко застосовуються незворотні перетворення булевої алгебри. На їх основі будуються, зокрема, сучасні алгоритми блокового симетричного шифрування та хеш-перетворення. В роботі [13] запропоновано метод ідентифікації, яких базується на використанні шифроблоків, за допомогою яких формується ланцюжок сеансових паролів абонента. Використання шифроблоків дозволяє на 2-3 порядки прискорити криптографічно-строгу ідентифікацію, але таке рішення має і низку недоліків: потребу генерувати і зберігати відразу всі сеансові паролі, вразливість до порушення синхронізації використання сеансових паролів.

В останні роки я якості незворотних задач для побудови механізмів генерації та перевірки сеансових паролів запропоновано використовували складні комбінаторні задачі [14]. Проте ці технології не знаходять застосування на практиці через складність генерації відкритого за закритого ключів.

Таким чином, до теперішнього часу, задача створення ефективного методу ідентифікації на основі криптографічного принципу “нульових знань”, що дозволяє радикально прискорити процес ідентифікації великої кількості віддалених абонентв інтегрованою системою не знайшла прийнятного для практичного застосування вирішення.

Мета досліджень

Мета дослідження полягає в прискоренні комп’ютерної реалізації криптографічного механізму перевірки коректності сеансового паролю віддаленого абонента при його ідентифікації на базі концепції “нульових знань” за рахунок застосування схеми формування паролю та його перевірки з несиметричним об’ємом обчислень.

Метод ідентифікації на основі криптографічних перетворень з несиметричним обсягом обчислень

Відповідно до поставленої мети, дослідження обмежуються організацією криптографічно строгої ідентифікації для окремого класу схем дистанційної інформаційної взаємодії, а саме тих, в яких інтегрована система надає певні інформаційні послуги чи ресурси великій кількості віддалених абонентів, котрі звертаються до системи в випадкові моменти часу. Фактично, мова йде про системи масового обслуговування віддалених абонентів. Характерною особливістю зазначеного класу схем дистанційної взаємодії є нерівномірність навантаження між її учасниками: домінуюча частина обчислювального навантаження по ідентифікації припадає на систему, яка має забезпечувати обслуговування запитів абонентів в реальному часі. Виходячи з цього, фактична швидкість ідентифікації віддалених абонентів визначається обчислювальною потужністю системи.

За цих умов одним із варіантів прискорення ідентифікації є її організація, що передбачає несиметричне обчислювальне навантаження для учасників дистанційної інформаційної взаємодії.

Тобто мова йде про таку організацію криптографічно строгої ідентифікації абонента, при якій левова частка обчислень реалізується на платформі абонента і відносно невелика – на комп'ютерній платформі системи. При цьому система може в режимі розділення часу проводити ідентифікацію декількох віддалених абонентів.

Для організації ідентифікації на основі теоретичної концепції нульових знань з несиметричним обчисленням навантаженням на систему та абонента, а також для підвищення рівня захищеності пропонується накласти додаткові умови на код, який система передає абоненту в процесі ідентифікації. Це необхідно для того, щоб система практично була нездатна отримати коректний пароль абонента. В принципі, вибір цих додаткових умов має забезпечувати, з одного боку, існування достатньо великої кількості кодів, що задовольняють цим умовам, а, з іншого, ймовірність випадкового отримання в результаті криптографічного перетворення коду, що задовольняє умовам має бути гранично малою. В рамках досліджень, обрано умову рівності хемінгової ваги коду певному числу h. Це означає, що система має надсилати абоненту для перевірки того, що від володіє механізмом генерації коректних паролів, n-розрядні коди, що містять в собі рівно h одиночних бітів.

Викладене вище покладено в основу запропонованого методу прискореної ідентифікації віддалених абонентів на основі криптографічної концепції "нульових знань", що теоретично забезпечує найбільший високий рівень захищеності. Метод регламентує порядок виконання двох базових процедур:

- реєстрації віддаленого абонента в системі;
- ідентифікація абонента системою безпосередньо перед початком кожного сеансу віддаленої взаємодії.

Розроблена процедура реєстрації абонента включає в себе виконання настпної послідовності дій:

1. Абонент довільним чином обирає два простих числа p і q, таким чином, щоб L = l·(p-1)·(q-1)+1 не було простим числом (l-ціле число). Абонентом обчислюється модуль M у вигляді добутку обраних ним чисел: M = p·q.

2. Абонент обирає W - найменший із подільників числа L. Обчислює значення H = L/W, яке зберігається абонентом в якості секретного ключа.

3. Абонент обирає ціле число h<<n.

4. Абонент надсилає свій відкритий ключ, що складається з трійки чисел <W,M, h >, системі.

5. Система приймає від абонента трійку чисел <W,M, h > і зберігає їх в пам'яті.

Функціонування описаної процедури реєстрації абонента може бути ілюстровано наступним прикладом. Нехай, абонентом обрано пару простих чисел p=11, q=17. Тоді при значенні l=1: L = (p-1)·(q-1)+1 = 10·16+1 = 161 = 7·23. Абонентом обчислюється модуль M = p·q = 11·17 = 187 = 1011 10112; розрядність модуля визначає чисельне значення n=8. Згідно п.2 процедури абонентом в якості параметра W обирається найменше з пари <7,23> простих подільників числа L=161: W=7. Абонент обчислює H=L/W= 161/7=23 і зберігає його в памяті в якості секретного ключа. У відповідності з п. 3 абонент обирає число h = 3. В рамках п.4 описаної процедури абонент надсилає трійку чисел <M=187, W=7, h=3> системі в якості свого відкритого ключа.

Процедура реєстрації віддаленого абонента системою включає в себе наступну послідовність дій:

1. Абонент надсилає системі запит на сеанс інформаційної взаємодії.

2. Система обирає код U, що містить рівно h двійкових розрядів і надсилає його абоненту.

3. Абонент обчислює код P сеансового паролю у вигляді: P = UH mod M і надсилає його системі.

4. Система обчислює значення G = PW mod M і порівнює його з кодом U : якщо обчислене значення дорівнює обраному системою коду U, тобто за умови G=P, ідентифікація вважається успішною. Відповідно, між системою та абонентом розпочинається сеанс віддаленої взаємодії.

Робота викладеної процедури ідентифікації може бути ілюстрована наступним прикладом. Нехай, у відповідь за запит абонента система генерує випадкове 8-розрядне число U, що містить рівно три одиничних біти, наприклад U = 10010012 =137. Це число надсилається абоненту. У відповідності з п.3 викладеної процедури, абонент обчислює значення сеансового паролю P = UH mod M = 13723 mod 187 = 103. Сеансовий пароль P=103 надсилається абонентом системі. Згідно п. 4 викладеної вище процедури, система обчислює G = 1037 mod 187 = 137 і порівнює отримане значення з обраним нею значенням U = 137. Оскільки G=P, то ідентифікація віддаленого абонента вважається успішною.

Можна показати, що запропонований метод задовольняє за всіма критеріями криптографічній концепції “нульових знань”. Дійсно, як цілком ясно з опису процедури ідентифікації, сеансовий пароль P змінюється в кожному сеансі віддаленої взаємодії абонента з системою. Механізм генерації коректних сеансових паролів забезпечується наявністю у абонента секретного ключа H. Наявний в системі криптографічний механізм перевірки коректності сеансових паролів визначається тим, що системі відома компонента W, така, що модулярне піднесення коректного паролю P в ступінь W завжди забезпечує отримання обраного системою числа U. Фактично, ця властивість забезпечується в силу справедливості узагальнення Ейлера малої теореми Ферма [2], згідно з якою, для довільного U<M виконується UW·H mod M = U. В силу того, що системі не відомий секретний код H, вона не здатна генерувати коректні сеансові паролі. Таким чином, доведено, що запропонований метод ідентифікації віддалених абонентів задовольняє теоретичній концепції “нульових знань”.

Оцінка ефективності

Ефективність запропонованого підходу може бути оцінена за двома традиційними для засобів захисту інформації критеріями:

- рівнем захищеності механізму криптографічно-строгої ідентифікації, який оцінюється обсягом ресурсів, потрібних для порушення захисту і незаконного доступу до ресурсів системи шляхом підробки паролю легального абонента;

- витратами часу на реалізацію процесу ідентифікації як стороні абонента, так і на стороні системи.

Рівень захищеності, що забезпечується схемою криптографічно строгої ідентифікації визначається обсягом обчислювальних ресурсів, потрібних для відтворення сеансового паролю, що забезпечує можливість незаконного входу в систему під іменем певного абонента.

Для криптографічно строгої ідентифікації, яка базується на теоретичній концепції нульових знань, окремо розглядається захищеність від спроб підбору коректного паролю самою системою і стороннім зловмисником.

В першому випадку, найбільш раціональна технологія підбору коректного паролю системою полягає в тому, що вона спробує підібрати такий пароль P′, що обчислений у вигляді код X=P′W mod M має рівно h одиниць.

Кількість μ n–розрядних кодів, що містять рівно h одиниць визначається відомою формулою Бернуллі :

$$\mu = C_n^h = \frac{n!}{h! \cdot (n-h)!}. \qquad (1)$$

Вважаючи на те, що на практиці значення n достатньо велике, для наближеного представлення його

факторіалу доцільно використати відому форму Стірлінга [15]. Після відповідних підстановок, формула (1) набуває наступного вигляду:

$$\mu \approx \left(\frac{n}{h}\right)^h \cdot \frac{1}{\sqrt{2 \cdot \pi \cdot \frac{h \cdot (n-h)}{n}}}. \qquad (2)$$

Приймаючи до уваги, що загальна кількість можливих n–розрядних кодів, які утворюються в результаті перетворення P′W mod M дорівнює 2n , ймовірність Q отримання в результаті цього перетворення коду, що містить рівно h одиниць визначається формулою:

$$Q = \frac{\mu}{2^n} = \left(\frac{n}{h}\right)^h \cdot \frac{1}{2^n \cdot \sqrt{2 \cdot \pi \cdot \frac{h \cdot (n-h)}{n}}} \quad . \quad (3)$$

В таблиці 1 наведені розраховані за формулами (2) та (3) значення μ та Q для різних значень n та h. При практичних застосуваннях число μ має бути достатньо великим, щоб практично виключалась можливість повторного вибору системою коду U. Разом з тим, ймовірність Q підбору системою коректного паролю має бути наскільки малою, щоб практично виключити можливість підбору системою коректного паролю абонента. Наприклад, при розрядності чисел n=4096 h=12 за даними таблиці 1 значення μ=1029, що дозволяє здійснювати 1029 сеансів віддаленої взаємодії системи та конкретного абоненту без повторень коду U. При цьому середня кількість обчислень модулярної експоненти P′W mod M для підбору коректного сеансового паролю P′ абонента складає Q-1 = 101204, що потребує обчислювальних ресурсів, обсяг яких далеко виходить за межі практично можливих.

Таблиця 1. Розрахункові значення μ - кількості n-розрядних кодів, що містять рівно h одиниць та ймовірності Q успішного підбору коректного сеансового ключа за одну спробу для типових для практики значень n та h.

n		*h*= 4	*h*=8	*h*=12	*h*=16
1024	μ	10^{9}	10^{16}	10^{22}	10^{28}
	Q	10^{-300}	10^{-295}	10^{-289}	10^{-281}
2048	μ	10^{10}	10^{18}	10^{26}	10^{32}
	Q	10^{-607}	10^{-599}	10^{-591}	10^{-585}
4096	μ	10^{11}	10^{20}	10^{29}	10^{37}
	Q	10^{-1222}	10^{-1213}	10^{-1204}	10^{-1196}
8192	μ	10^{12}	10^{22}	10^{33}	10^{42}
	Q	10^{-2454}	10^{-2444}	10^{-2433}	10^{-2424}

Таким чином, показано, що система реально не здатна підробити коректний пароль конкретного користувача, тобто за критерієм рівня захищеності запропоноване рішення повною мірою задовольняє теоретичній концепції "нульових знань".

Основна перевага запропонованого рішення полягає в тому, що воно забезпечує суттєве пришвидшення криптографічно строгої ідентифікації у порівнянні з відомими методами. При цьому, з огляду на те, що запропоноване рішення орієнтоване для швидкої ідентифікації великої кількості абонентів системи колективного доступу, критичним є витрати часових ресурсів саме системою. Відповідно, в якості критерію часової ефективності запропонованого методу доцільно розглядати коефіцієнт β, який визначається співвідношенням часу Ts що витрачається системою для ідентифікації абоненту в відомих методах до часу Ts′, який витрачається системою в запропонованому методі:

$$\beta = \frac{T_S}{T_S'}. \qquad (4)$$

В більшості відомих схем криптографічно строгої ідентифікації, зокрема таких, як метод Guillou-Quisquater [3] перевірка коректності паролю потребує $6 \cdot n^3/r$ процесорних операцій, тобто $T_S = 6 \cdot n^3 \cdot t_0/r$, де t_0 – час виконання процесорної операції типу додавання і зсуву.

В запропонованому методі, для перевірки коректності сеансового паролю абонента система виконує модерне експоненціювання PW mod M , причому компоненти P та M мають розрядність n, а довжина k коду експоненти W значно менша за n: k<<n. Відповідно, при реалізації модулярного експоненціювання за класичним алгоритмом [2], середня кількість мультиплікативних модулярних операцій над n-розрядними числами становить 1.5·k. За умови реалізації кожної з таких операцій за алгоритмом модулярного множення Монтгомері, час їх виконання дорівнює 2·n2·t0/r. Відповідно, чисельне значення часу Ts′ який витрачається системою для ідентифікації абоненту в запропонованому методі визначається у вигляді: TS′ = 3·k·n2·t0/r. З урахуванням наведеного, чисельне значення коефіцієнту β прискорення ідентифікації віддалених абонентів при використанні запропонованого методу в порівнянні з відомими визначається наступним виразом:

$$\beta = \frac{T_S}{T_S'} = \frac{6 \cdot n^3 \cdot \frac{t_0}{r}}{3 \cdot k \cdot n^2 \cdot \frac{t_0}{r}} = 2 \cdot \frac{n}{k} \quad . \quad (5)$$

Чисельне значення коефіцієнта β прискорення ідентифікації, яке досягається використанням запропонованого методу може бути визначене шляхом підстановки в формулу (5) типових для практичних застосувань значень n та k. Враховуючи, що реальні значення розрядності n чисел, лежать в діапазоні від 2048 до 8192, а довжина k не перевищує десяти, значення коефіцієнту β прискорення ідентифікації лежить в межах від 400 до 1600. При цьому в якості основного чинника прискорення ідентифікації на стороні системи виступає мала розрядність експоненти, що використовується для перевірки коректності сеансового паролю віддаленого абонента.

Проведені експериментальні дослідження, в цілому, підтвердили наведені вище теоретичні оцінки часової ефективності запропонованого методу ідентифікації, що реалізує криптографічну концепцію “нульових знань”.

Висновки

Проведені дослідження, націлені на прискорення комп’ютерної реалізації ідентифікації віддалених абонентів у відповідності з криптографічною концепцією “нульових знань” дозволити отримати наступні результати.

Теоретично обґрунтовано, розроблено та досліджено метод ідентифікації віддалених абонентів системою на базі криптографічної концепції “нульових знань”, який відрізняється тим, що код доступу, який генерується системою має фіксовану кількість одиничних бітів, а також тим, що обсяг обчислень, які реалізуються на стороні абонента та системи відрізняються на порядки через різну довжину коду показника базової обчислювальної операції – модулярного експоненціювання, за рахунок чого на порядки скорочується час перевірки коректності сеансового паролю абонента системою, яка одночасно обслуговує декілька абонентів.

Теоретично доведено, що за рахунок спеціальних властивостей коду доступу, система самостійно практично не здатна самостійно генерувати коректний пароль абонента.

З використанням математичних моделей доведено і експериментально підтверджено, що запропонований метод дозволяє на 2-3 порядки скоротити витрати часу на ідентифікації на стороні системи, що дозволяє одночасно виконувати ідентифікацію великої кількості абонентів одночасно.

Розроблений метод орієнтовано для ідентифікації з високим рівнем захисту в інтегрованих системах колективного доступу великої кількості віддалених абонентів.

Література

1. 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.

2. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed.John Wiley, 1996 - 758 pp.

3. Asimi Y. Strong zero-knowledge authentication based on the session keys (SASK) / Y.Asimi, A. Amghar, A. Asimi, Y. Sadgi // International Journal of Network Security & Its Applications (IJNSA).- 2015.- Vol.7, - №.1,- P.51-66.

4. Bardis N. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution / N.Bardis, N.Doukas, O. Markovskyi // International Journal of Multimedia Intelligence and Security.- 2010.- №.4,- P. 363-377.

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. Menezes Alfred, Handbook of Applied Cryptography. / Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone // CRC Press. – 2001. – 780 p.

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. Верба О.А. Метод криптографічно строгої ідентифікації з блокуванням повторного використання паролів / О.А. Верба, І.В. Дайко // // Проблеми інформатизації та управління. - 2024.- № 2 (78).- С.4-13. DOI: 10.18372/2073-4751.78.18955

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

10. Markovskyi Oleksandr. Fast Zero-Knowledge Identification Method with Password Reuse Blocking / Oleksandr Markovskyi, Katerina Bojko, Spiros Kostoudas, Nikolas Bardis // 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 2024, P. 142-146, DOI: 10.1109/DESSERT65323. 2024.11122142.

11. 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.

12. Марковський О.П. Метод швидкого обчислення експоненти на полях Галуа GF(2n) для криптографічних застосувань /О.П. Марковський, С.С. Нікольський //. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2025.- Вип. 58. – С. 188-196. DOI: 10.36910/6775-2524-0560-2925-58-23/

13. Bardis N.G. Identification Method Based on Block Ciphers / N.G. Bardis, N/ Doukas, O.P. Markovskyi // International Conference on Control, Artificial Intelligence, Robotics & Optimazation (ICCAIRO) . Praque, Czech Republic 20-22 May 2018.- IEEE.- 2018.- P. 307-311.

14. Aquilar C.. A new zero-knowledge code based identification scheme with reduced communication / C. Aquilar, P. Gaborit, J. Schrec //. IEEE Information Theory Workshop 16-20 Oct. 2011 .-2011.- P.648-652.
DOI: 10.1109/ITW.2011.6089577.

15. Santosh S. Venkatesh. Theory of Probability: Exploration and Applications. Cambridge University Press: 2012.- 827 p.

Марковський О.П., Дайко І.В., Григораш Ю.В.

ПІДХІД ДО РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНОЇ КОНЦЕПЦІЇ "НУЛЬОВИХ ЗНАНЬ" ДЛЯ ПРИСКОРЕНОЇ ІДЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ

У статті пропонується метод прискореної ідентифікації в рамках криптографічної концепції "нульових знань", орієнтований на використання в системах, які взаємодіють з великою кількістю віддалених абонентів. Скорочення часу ідентифікації системою віддаленого абонента досягається за рахунок організації несиметричного обчислювального навантаження на систему та абонента в процесі реалізації запропонованої процедури криптографічно строгої ідентифікації. Розроблено формалізовані процедури реєстрації абонента та його ідентифікації перед початком сеансу віддаленої взаємодії з системою. Робота процедур проілюстрована прикладами.

Теоретично доведено та експериментально підтверджено, що запропонований підхід дозволяє на 2-3 порядки скоротити час ідентифікації абонента системою в порівнянні з відомими методами криптографічно строгої ідентифікації.

Ключові слова: *ідентифікація на основі концепції "нульових знань", криптографічно строга ідентифікація, модулярне експоненціювання, криптографія з відкритим ключем.*

Markovsky O.P., Daiko I.V., Grygorash Y. V.

AN APPROACH TO IMPLEMENTATION OF THE ACCELERATED ZERO KNOWLEDGE IDENTIFICATION OF REMOTE ABONENTS

The article proposes a method of accelerated zero knowledge identification, aimed at use in systems that interact with a large number of remote abonents. Reduction of the system identification time of a remote abonent is achieved due to the organization of an asymmetric computing load on the system and the abonent in the process of implementing the proposed procedure of cryptographically strong identification.

Formalized procedures for abonent registration and identification before the start of a remote interaction session with the system have been developed. The work of the procedures is illustrated by examples.

It is theoretically proven and experimentally confirmed that the proposed approach allows to reduce the time of abonent identification by the system by 2-3 orders of magnitude compared to known methods of cryptographically strong identification.

Keywords*; Zero-Knowledge Identification, cryptographically strong identification, modular exponentiation, open key cryptography.*

Стаття подана до редакції: 13/03/2026
Стаття прийнята до опублікування: 16/03/2026
Стаття опублікована: 27/04/2026