УДК 004.052.42

О.П. Марковський [1], канд. техн. наук,
Захаріудакіс Лефтеріс [2], **В.Р. Максимук** [1]
[1] Національний технічний університет України
«Київський політехнічний університет»
(Україна, 03056, Київ, пр-т Перемоги, 37, ком. 2003,
тел. (044) 2049291; e-mail: markovskyy@i.ua; vikamaksymuk@gmail.com),
[2] Навчальний центр ім. Макарія
(Кіпр, Нікозія, compusci@cytanet.com.cy)

Використання алгебри полів Галуа для реалізації концепції «нульових знань» при ідентифікації та автентифікації віддалених користувачів

Запропоновано новий підхід до реалізації теоретично строгої, у відповідності з концепцією «нульових знань», ідентифікації та автентифікації віддалених користувачів. Запропонований підхід полягає в використанні незворотних перетворень в алгебрі полів Галуа. Це дозволяє прискорити процес ідентифікації користувачів як при програмній, так і при апаратній реалізації. Досліджено циклічні властивості операції піднесення до степеня на полях Галуа спеціальних класів. На основі цих властивостей розроблено процедури реєстрації та ідентифікації користувачів, функціонування яких ілюстроване числовими прикладами. Теоретично та експериментально доведено, що запропонований підхід забезпечує прискорення процесів ідентифікації на один-два порядки при апаратній реалізації.

К л ю ч о в і с л о в а: концепція «нульових знань», ідентифікація віддалених користувачів, автентифікація користувачів, незворотні перетворення на полях Галуа.

Предложен новый подход к реализации теоретически строгой, в соответствии с концепцией «нулевых знаний», идентификации и аутентификации удаленных пользователей. Предложенный подход состоит в использовании необратимых преобразований в алгебре полей Галуа. Это позволяет ускорить процесс идентификации пользователей как при программной, так и при аппаратной реализации. 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.

К л ю ч е в ы е с л о в а: концепция «нулевых знаний», идентификация удаленных пользователей, аутентификация пользователей, необратимые преобразования на полях Галуа.

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, важливе місце серед яких 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 чергу, 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 зруйнування існуючих механізмів контролю доступу до інформації. Це об'єктивно вимагає здійснення 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 важливою з огляду особливостей сучасного етапу розвитку інформаційних та комп'ютерних технологій.

Аналіз існуючих засобів реалізації строгої ідентифікації. Проблема ефективної ідентифікації та автентифікації є одною з базових задач захисту інформації. Тому до теперішнього часу створено і використовується широкий арсенал методів та засобів ідентифікації віддалених абонентів. При цьому в якості критерію ефективності засобів ідентифікації віддалених користувачів розглядається стійкість системи до спроб несанкціонованого проникнення в систему користувачів, а також об'єм ресурсів, які витрачаються на реалізацію процесу ідентифікації. Сучасні сервіси безпеки функціонують в розподілених мережах, де необхідно враховувати імовірність появи загрози як з локального, так і з мережевого середовища. В

основі переважної більшості методів ідентифікації віддалених користувачів лежить доказ знання користувачем якоїсь інформації.

Методи ідентифікації та автентифікації можна розділити на два класи: з використанням паролей («слабка» ідентифікація) і на основі теоретичної концепції «нульових знань» («строга» ідентифікація) [1]. Ідентифікація на основі паролей вважається «слабкою» виходячи з того, що при її використанні порушується принцип єдиного власника секретних даних.

Сутність концепції нульових знань полягає в тому, що для доведення своєї автентичності 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. Суттєвим є те, що при кожному зверненні до системи користувачем генерується новий сеансовий пароль.

Таким чином, концепція нульових знань в теоретичному плані найбільш повною мірою відповідає сформульованим вище вимогам щодо системи ідентифікації абонентів. Концепція нульових знань передбачає використання теоретично незворотних криптографічних перетворень. Це означає, що існує алгоритм перетворення в прямому напрямку, але принципово неможливим є аналітичне віднаходження алгоритму зворотного перетворення.

В сучасних умовах і у найближчій перспективі потрібний для практики рівень надійності ідентифікації може бути забезпечений лише методами, що спираються на концепцію нульових знань [2]. Найбільш відомими методами, які реалізують цю концепцію є FFSIS (Feige Fiat Shamir Identification Scheme) [3], методи Шнора (Schnorr) та Гіллоу—Квіскватера (Guillou—Quisquater) [1]. Базовими обчислювальними операціями для FFSIS є $A^2B \bmod m$, а для методів Шнора і Гіллоу—Квіскватера — $A^eB^v \bmod m$. Враховуючи те, що задля забезпечення потрібного рівня захищеності розрядність чисел становить 2048 або 4096, швидкість ідентифікації обмежується значною обчислювальною складністю цих операцій і, відповідно, виникає необхідність в її зменшенні.

Метою дослідження є зменшення обчислювальної складності процесу ідентифікації при забезпеченні високого рівня захищеності. Крім того, метод FFSIS, обчислювальна реалізація якого потребує найменших ресурсів, передбачає близько 20 циклів обміну даними між системою та користувачем в одному сеансі ідентифікації. Це суттєвим чином сповільнює процес ідентифікації віддалених користувачів. В роботі [4] запропоновано більш ефективний в обчислювальному плані метод реалізації концепції нульових знань. Проте саме використання традиційної арифметики

з переносами між окремими розрядами значно ускладнює можливості ефективної апаратної реалізації ідентифікації сервером системи.

Таким чином, основний недолік існуючих методів реалізації концепції нульових знань полягає в значній обчислювальній складності їх базових обчислювальних процедур.

Розробка математичного підґрунтя. Для досягнення поставленої мети досліджено циклічні властивості операції піднесення до степеня на полях Галуа, утворюючий поліном $M(x)$ яких є поліноміальним добутком 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 широкого кола механізмів криптографічного захисту використовується модулярне піднесення до степеня $A^E \bmod M$, в алгебрі скінчених полів Галуа для криптографічних застосувань в якості базової застосовується операція піднесення до степеня $A|^E \text{ rem } M$ на полях [5].

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

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

де $\otimes$ — операція поліноміального множення, або множення без переносів (Multiplication Without Carry (MWC)); rem — операція редукції на полі Галуа, тобто віднаходження залишку при поліноміальному діленні результату множення без переносів на утворюючий поліном M поля.

Якщо $g(x)$ – простий поліном степеня 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 наступна рівність [4] :

$$u|^{h+1} \text{ rem } g = u. \qquad (1)$$

Наприклад, для простого полінома $g(x) = x^6 + x^4 + x^2 + x + 1$ степеня $d = 6$, якому співвідноситься двійкове число 87, а $h = 63$, для будь-якого $u(x) = x^5 + x^3 + x + 1$, що співвідноситься з числом $u = 43$, виконується наступне: $43|^{64} \text{ rem } 87 = 43$.

Якщо утворюючий поліном $M(x)$ степеня r являє собою добуток двох простих поліномів $p(x)$ степеня v і $g(x)$ степеня d, тобто $M(x) = p(x) \otimes g(x)$, $r = v + d$, і при цьому 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, $u \le h = 2^d - 1$, справедлива рівність

$$(u \otimes p)|^{h+1} \text{ rem } m = u \otimes p. \qquad (2)$$

Наприклад, якщо $p(x)=x^3+x^2+1$ — простий поліном степеня $v=3$, якому відповідає число $p=13$, для якого $l=2^3-1=7$, і $g(x)=x^5+x^4+x^3+x+1$ — простий поліном степеня $d=5$, якому відповідає число $g=59$, для якого $h=2^5-1=31$, то добуток цих поліномів має вигляд $M(x)=p(x)\otimes g(x)=x^8+x^3+x^2+x+1$ і співвідноситься з числом $m=271$. Якщо вибрати число u таким чином, що $0<u\le h-1$, зокрема $u=28$, то $u\otimes p=140$. Тоді $(u\otimes p)|^{h+1}\ \mathrm{rem}\ m=(28\otimes 13)|^{32}\ \mathrm{rem}\ 271=140$.

Аналогічно для будь-якого полінома $w(x)$, що належить полю $GF(2^d)$ та співвідноситься з числом w так, що $w\le l=2^v-1$, справедливо наступне:

$$(w\otimes g)|^{l+1}\ \mathrm{rem}\ m=w\otimes g. \qquad (3)$$

Якщо в рамках наведеного прикладу вибрати довільне w менше за l $(0<w<l)$, наприклад $w=5$, то отримаємо $w\otimes g=5\otimes 59=215$. Відповідно $(w\otimes g)|^{l+1}\ \mathrm{rem}\ m=(5\otimes 59)|^{8}\ \mathrm{rem}\ 271=215$, тобто дорівнює згідно (3) $w\otimes g$. Доведення $(u\otimes p)|^{h+1}\ \mathrm{rem}\ m=u\otimes p$ можна виконати розкладенням лівої частини на дві складові:

$$(u\otimes p)|^{h+1}\ \mathrm{rem}\ m=u|^{h+1}\ \mathrm{rem}\ m\otimes p|^{h+1}\ \mathrm{rem}\ m. \qquad (4)$$

Якщо модуль $M(x)$ утворено в результаті поліноміального множення простого полінома $p(x)$ степеня v і простого полінома $g(x)$ степеня d $(M(x)=p(x)\otimes g(x))$ за умови, що $v<d$, то $p<h$ і згідно (1) для нього справедливо $p|^{h+1}\ \mathrm{rem}\ g=p$. Іншими словами, p степеня $h+1$ можна представити у вигляді суми добутку цілого λ на g та p: $p|^{h+1}=g\otimes\lambda+p$. З іншого боку, $g\otimes\lambda+p$, як степінь p, ділиться на p. З цього слідує, що і $g\otimes\lambda$ ділиться на p, звідки випливає, що $g\otimes\lambda$ ділиться на p і на g, а значить, $g\otimes\lambda$ може бути представлено у вигляді $g\otimes\lambda=g\otimes p\otimes\xi$, де ξ — ціле число, відповідно $(g\otimes\lambda)\ \mathrm{rem}\ m=0$. Таким чином, другу складову виразу (4) можна подати у вигляді $p|^{h+1}\ \mathrm{rem}\ m=(m\otimes\xi+p)\ \mathrm{rem}\ m=p$. Після підстановки отриманого виразу в (4) запишемо:

$$(u\otimes p)|^{h+1}\ \mathrm{rem}\ m=u|^{h+1}\ \mathrm{rem}\ m\otimes p=(u|^{h+1}\otimes p)\ \mathrm{rem}\ m.$$

Оскільки $u<h$ і для нього згідно (1) виконується рівність $u|^{h+1}\ \mathrm{rem}\ g=u$, з цього випливає, що u степеня $h+1$ можна представити у вигляді $u|^{h+1}=g\otimes y+u$. Виконавши відповідну підстановку в (4), отримаємо наступне:

$$(u\otimes p)|^{h+1}\ \mathrm{rem}\ m=(((g\otimes\psi)\otimes u)\otimes p)\ \mathrm{rem}\ m=$$

$$=(g\otimes p\otimes\psi\otimes p\otimes u)\ \mathrm{rem}\ m=p\otimes u,$$

що й потрібно було довести.

Для доведення рівності (3) доцільно окремо розглянути дві її мультиплікативні складові: $(w \otimes g)|^{l+1} \text{ rem } m = w|^{l+1} \text{ rem } m \otimes g|^{l+1} \text{ rem } m$. Можна довести, що $g|^{l+1} \text{ rem } m = g$. Оскільки $g > p$, то g завжди може бути представлено у вигляді $g = \kappa \otimes p \otimes \varphi$, де κ та φ — цілі числа. Відповідно $g|^{l+1} \text{ rem } m$ можна представити у вигляді $g \otimes (\kappa \otimes p \oplus \varphi)|^l \text{ rem } m = g \otimes (\chi_1 \otimes p \oplus ... \oplus \chi_v \otimes p \oplus \varphi|^l) \text{ rem } m$, де $\chi_1 ... \chi_v$ — цілі числа. Після розкриття дужок, враховуючи, що $g \otimes \chi_\gamma \otimes p \text{ rem } m = 0$, $\forall \gamma \in \{1, ..., \upsilon\}$, можна отримати $g|^{l+1} \text{ rem } m = g \otimes \varphi|^l \text{ rem } m$. Оскільки $\varphi < p$, згідно (1) справедливо наступне: $\varphi|^l \text{ rem } p = 1$. Це означає, що $\varphi|^l$ може бути представлене у вигляді суми одиниці та добутку цілого числа ε на p: $\varphi|^l = \varepsilon \otimes p \otimes 1$. Відповідно $g \otimes \varphi|^l \text{ rem } m = g \otimes (\varepsilon \otimes p \oplus 1) \text{ rem } m = (g \otimes \varepsilon \otimes p \oplus g) \text{ rem } m = g$.

Другу мультиплікативну компоненту добутку $w|^{l+1}$ можна подати у вигляді суми $w \oplus \varsigma \otimes p$. Це випливає з того, що $w < l$ і для нього виконується (1), тобто $w|^{l+1} \text{ rem } p = w$. З урахуванням цього отримуємо

$$(w \otimes g)|^{l+1} \text{ rem } m = ((w \oplus ... \oplus \varsigma \otimes p) \otimes g) \text{ rem } m = w \otimes g,$$

що й потрібно було довести.

З доведеного прямо випливає, що за умови формування утворюючого полінома $M(x)$ у вигляді поліноміального добутку двох простих поліномів, $p(x)$ степеня v і $g(x)$ степеня d ($M(x) = q(x) \otimes g(x)$) процес піднесення до степеня породжує два цикли: перший з періодом $h = 2^d - 1$ та другий з періодом $l = 2^v - 1$. При цьому значення v і d можуть обиратися абонентом довільним чином і триматися в секреті від системи надання ресурсів, якій повідомляється тільки значення утворюючого полінома $M(x)$ поля.

Таким чином, знання однією зі сторін процесу ідентифікації періоду повторення операції піднесення до степеня дозволяє будувати ефективні алгоритми ідентифікації в рамках криптографічно строгої концепції нульових знань.

Метод строгої ідентифікації абонентів з використанням алгебри полів Галуа. Базуючись на встановленій властивості пропонуємо метод ідентифікації віддалених користувачів, який реалізує концепцію нульових знань — теоретично строгої ідентифікації. Метод включає дві базові процедури: реєстрації користувача та безпосередньо його ідентифікації системою.

Запропонована процедура реєстрації передбачає наступну послідовність дій користувача:

1. Отримання від системи її відкритого закриваючого ключа K_c.

2. Довільний вибір пари простих поліномів, $p(x)$ та $g(x)$, з різними степенями: $p(x) = x^v + p_{v-1}x^v + ... + p_1 x + p_0$ степеня v та $g(x) = x^d +$

$+ g_{d-1}x^{d-1} + ... + g_1x + g_0$ степеня d, де $p_0, p_1, ..., p_{v-1} \in \{0, 1\}$, $g_0, g_1, ...$ $..., g_{d-1} \in \{0,1\}$, при цьому $d > v$.

3. Формування полінома $M(x)$ 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. Вибір випадкового числа β ($0 < \beta < 2^d$) та обчислення другої компоненти α відкритого ключа користувача у вигляді $\alpha = p|^{\beta}$ rem m.

5. Шифрування відкритим закриваючим ключем K_c двох компонент відкритого ключа користувача, m та β, і відсилання їх до системи.

6. Система з використанням секретного відкриваючого ключа K_o відновлює значення обох компонент, m і β, ключа користувача, після чого зберігає їх в захищеній пам'яті.

Наведена процедура реєстрації може бути ілюстрована наступним прикладом. У відповідності з кроком 2 користувач вибирає простий поліном степеня 3 ($v = 3$) $p(x) = x^3 + x^2 + 1$, який співвідноситься з числом $p = 11$, та простий поліном степеня 5 ($d = 5$) $g(x) = x^5 + x^4 + x^3 + x + 1$, з яким співвідноситься число $g = 59$. Далі користувач формує утворюючий поліном $M(x)$ як поліноміальний добуток вибраних простих поліномів, $M(x) = p(x) \otimes g(x) = x^8 + x^7 + x^4 + x^2 + 1$, який співвідноситься з числом $m = 405$. Це число шифрується відкритим ключем K_c та відправляється в систему.

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 полінома $k(x)$ на поліном $p(x)$: $q(x) = k(x) \otimes p(x)$.

2. Користувач довільним чином вибирає число $U < 2^d$ та виконує піднесення до степеня на полі Галуа з базовим поліномом $M(x)$: $R = q|^U$ 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 $\rho = q|^E$ rem M піднесенням q до степеня E в полі Галуа з базовим поліномом $M(x)$. Далі системою обчислюється добуток в полі Галуа: $\eta = \rho \otimes R$ rem M. Отриманий результат η порівнюється з q: якщо $\eta = q$, то ідентифікація користувача вважається успішною.

Запропонована процедура ідентифікації може бути описана наступним чином. Згідно з пунктом 1 користувач вибирає довільне k, менше за $2^5 = 32$. Нехай вибрано число $k = 18$. Вибране число k поліноміально множиться на число p: $q = k \otimes p = 18 \otimes 11 = 166$. Користувач довільним чином

вибирає $U < 2^{32}$, наприклад $U = 17$, та виконує обчислення експоненти: $R = q\ |^{U}$ rem $M = 166\ |^{17}$ rem $405 = 173$. Далі, у відповідності з пунктом 3, користувач обчислює $E = 2^{32} - U = 2^5 - 17 = 15$, після чого відсилає трійку чисел $< q, R, E > = < 166, 173, 15 >$ в якості сеансового паролю системи. Система, отримавши від користувача сеансовий пароль, у відповідності до пункту 4 спочатку обчислює $\rho = q\ |^{E}$ rem $M = 166|^{15}$ rem $405 = 210$, а потім поліморфний добуток: $\eta = \rho \otimes R \text{ rem } M = 210 \otimes 173 \text{ rem } M = 166$. Оскільки $\eta = g$, ідентифікацію виконано успішно.

Метод строгої автентифікації абонентів з використанням алгебри полів Галуа. Запропонований вище підхід до реалізації ідентифікації віддалених користувачів в рамках криптографічно строгої концепції нульових знань з використанням алгебри полів Галуа може бути модифікованим для реалізації задачі автентифікації віддалених користувачів. Процедура автентифікації, на відміну від ідентифікації, дозволяє не тільки гарантувати взаємодію системи з авторизованим користувачем, але й надає користувачеві механізми, які дозволяють впевнитися в тому, що він взаємодіє дійсно з системою.

Запропонована процедура реєстрації передбачає наступну послідовність дій.

1. Користувач отримує від системи її відкритий закриваючий ключ K_c.

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

3. Користувач формує поліном $M(x)$ у вигляді поліноміального добутку вибраних двох простих 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 $\alpha = p\ |^{\beta}$ rem m.

5. Користувач вибирає довільне число $\eta < 2^{d+v} - 2^{d+1}$. Це число η являє собою третю компоненту ключа користувача. Користувач обчислює значення коду $\chi = 2^{d+v} - 2^d - 2^v + 1 - \eta$, яке зберігається в пам'яті користувача.

6. Три компоненти, m, α та η, ключа користувача шифруються відкритим закриваючим ключем K_c і відсилаються системі.

7. Система з використанням секретного відкриваючого ключа K_o відновлює значення трьох компонентів, m, α та η, ключа користувача, після чого зберігає їх в захищеній пам'яті.

Запропонована процедура реєстрації може бути ілюстрована наступним прикладом. У відповідності з пунктом 2 користувач вибирає простий поліном степеня 3 ($v = 3$), $p(x) = x^3 + x^2 + 1$, який співвідноситься з числом $p = 11$, та простий поліном степеня 5 ($d = 5$), $g(x) = x^5 + x^4 + x^3 + x + 1$, якому співвідноситься число $g = 59$. Згідно з пунктом 2 користувач формує утворюючий поліном $M(x)$ як поліноміальний добуток вибраних простих поліномів, $M(x) = p(x) \otimes g(x) = x^8 + x^7 + x^4 + x^2 + 1$, який співвідноситься з числом $m = 405$. Згідно з пунктом 4 процедури реєстрації користувач випадковим чином обирає число $\beta = 18$ та обчислює другу компоненту α ключа: $\alpha = p|^{\beta} \text{ rem } m = 11|^{18} \text{ rem } 405 = 49$. Згідно з пунктом 5 запропонованої процедури користувач обирає довільне η, менше $2^{d+v} - 2^{d+1} = 192$. Нехай вибране значення η дорівнює 18. Користувач обчислює значення $\chi = 2^{d+v} - 2^d - 2^v + 1 - \eta = 218 - 18 = 200$. Трійка компонентів ключа користувача $< 405, 49, 18 >$ шифрується відкритим ключем K_c системи та відправляється в систему.

Розроблена процедура одного циклу автентифікації віддаленого абонента передбачає виконання наступної послідовності дій.

1. Користувач ініціює звернення до системи.

2. Система формує випадкове число r, з використанням компонентів m та η ключа користувача обчислює значення $\gamma = r \mid^{\eta} \text{rem } m$. Коди r та γ відсилає користувачеві.

3. Користувач приймає від системи код r та γ. Для перевірки того, що він працює дійсно з системою, обчислює $\sigma = r \mid^{\chi} \text{rem } m$. Якщо $\sigma \otimes \gamma = r$, тобто поліноміальний добуток обчисленого σ на отриманий код γ дорівнює отриманому від системи числу r, то користувач впевнюється в тому, що сторона, яка надіслала йому коди r та γ, дійсно знає компоненти його ключа m та η, тобто є системою.

4. Впевнившись, що комутація відбувається дійсно з системою, користувач віднаходить число w таке, для якого виконується умова $rw \bmod (2^d - 1) = \beta$.

5. Користувач обчислює сеансовий пароль ρ у вигляді $\rho = p|^{\rho} \text{ rem } m$, після чого шифрує за допомогою відкритого ключа K_c отриманий код ρ та надсилає його системі.

6. Система, отримавши зашифрований сеансовий пароль ρ, розшифровує його своїм секретним відкриваючим ключем K_o та обчислює $y = \rho|^{r} \text{ rem } M$. Отримане значення y порівнюється з другою компонентою α відкритого ключа цього користувача: якщо ці коди співпадають, тобто $y = \alpha$, то сеанс автентифікації вважається успішним і користувачеві надається доступ до ресурсів системи.

Робота запропонованої процедури одного сеансу ідентифікації може бути ілюстрована наступним прикладом, який фактично є продовженням попереднього.

У відповідності з пунктом 2 процедури у відповідь на звернення користувача система випадковим чином вибирає число $r = 28$ і обчислює значення $\gamma = r \,|^{\eta} \operatorname{rem} m = 28|^{18} \operatorname{rem} 405 = 38$. Отримані значення, $r = 28$ та $\gamma = 38$, система пересилає користувачеві.

Користувач приймає від системи надіслані йому коди $r = 28$ та $\gamma = 38$. Для того щоб впевнитися, що сторона, яка надіслала йому ці коди, дійсно знає його ключ, тобто є системою, користувач згідно з пунктом 3 процедури обчислює $\sigma = r \,|^{\chi} \operatorname{rem} m = 28 \,|^{200} \operatorname{rem} 405 = 117$. Далі користувач обчислює поліноміальний добуток $\sigma \otimes \gamma = 117 \otimes 38 = 28$. Оскільки значення обчисленого добутку співпадає з отриманим кодом $r = 28$, користувач фактично ідентифікує сторону, що веде з ним інформаційний обмін, як систему, що знає його реєстраційний ключ.

У відповідності до пункту 4 даної процедури користувач віднаходить таке w, для якого виконується умова $28\ w \bmod 31 = 18$. Ця умова виконується для $w = 25$. Згідно з пунктом 5 користувач обчислює сеансовий пароль ρ у вигляді $\rho = p \,|^{\rho} \operatorname{rem} m = 11 \,|^{25} \operatorname{rem} 405 = 245$ і надсилає його системі. Згідно з пунктом 6 система, отримавши зашифрований сеансовий пароль ρ, розшифровує його своїм секретним відкриваючим ключем K_o та обчислює $y = \rho \,|^{r} \operatorname{rem} m = 245 \,|^{28} \operatorname{rem} 405 = 49$. Це значення порівнюється з другою компонентою α ключа користувача. Оскільки обчислене значення $y = 49$ співпадає зі значенням другої компоненти реєстраційного ключа цього конкретного користувача $\alpha = 49$, то система успішно його ідентифікує.

Оцінка ефективності. Як і для будь-якого механізму криптографічного захисту даних, ефективність запропонованого методу ідентифікації віддалених користувачів оцінюється за двома базовими критеріями: рівнем захисту та часовими характеристиками реалізації. Оцінку рівня захищеності доцільно виконувати з двох позицій: з позиції третьої сторони, яка може мати доступ до каналу обміну ідентифікаційною інформацією, але не знає коду утворюючого полінома $M(x)$ поля Галуа, та з позицій зловмисника, що має доступ до даних, які зберігаються в системі, і зокрема до кодів $M(x)$, $p(x)$ та $g(x)$.

Очевидно, що для того щоб виконати успішний підбір коректного паролю користувача, потрібно знати простий поліном $g(x)$, а також степень v іншого простого полінома $p(x)$. Найдоцільніша технологія підбору компоненти паролю $p(x)$ для стороннього зловмисника полягає в перехопленні коду $q(x) = k(x) \otimes p(x)$ та розкладанні його на співмножники. Важ-

ливим при цьому є те, що у зловмисника практично відсутній критерій коректності розкладання. Ще одна особливість задачі розкладання коду $q(x)$ на співмножники полягає в тому, що один з співмножників не є простим, що потенційно збільшує обсяг перебору. Кількість можливих простих поліномів швидко зростає зі збільшенням їх степеня. Та уже при степені 29 кількість простих поліномів перевищує $18 \cdot 10^6$. На практиці степень полінному становить сотні і відповідно задача перебору простих поліномів виходить далеко за рамки технічних можливостей сучасних комп'ютерів.

Для зловмисника, що має доступ до ідентифікаційної інформації, яка зберігається в системі, задача відтворення коректного паролю зводиться до задачі розкладання відомого полінома $M(x)$ на два простих множника, $p(x)$ та $g(x)$, з різними степенями. Як зазначалося вище, розв'язок такої задачі шляхом перебору для реальних степенів поліномів виходить далеко за межі технічних можливостей сучасних комп'ютерних систем.

Основна перевага запропонованого способу ідентифікації віддалених абонентів в рамках концепції нульових знань полягає в тому, що використання операції піднесення до степеня в полях Галуа на відміну від модулярного піднесення до степеня дозволяє значно прискорити час виконання програм та спростити апаратну реалізацію. Наведемо 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 піднесення до квадрату n-розрядного числа в традиційній алгебрі потребує виконання $(n/r)^2/2$ операцій процесорного множення;

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

в операціях на полях Галуа не використовується перенос, що значно прискорює їх виконання в порівнянні з операціями традиційної алгебри, для яких формування міжрозрядних переносів для розрядностей 2018 і 4096, що здебільшого використовуються на практиці, потребує значних затрат часових та апаратних ресурсів.

В роботі [6] показано, що операція піднесення до степеня в полях Галуа виконується на два-три порядки швидше у порівнянні з модулярним піднесенням до степеня, яке є базовою для існуючих методів Guillou—Quisquater [1] та Schnorr [1] реалізації ідентифікації в рамках концепції

нульових знань. Важливою перевагою запропонованого методу є те, що на відміну від відомих методів, і, насамперед, методу FESIS, в ньому використовується лише один цикл передачі даних.

Експериментальні дослідження показали, що при апаратній реалізації ідентифікації засобами на програмованих матрицях досягається значне прискорення процедур ідентифікації в порівнянні з FESIS. Зокрема, моделювання засобами VHDL показало зростання швидкості ідентифікації на один-два порядки.

Висновки

На основі отриманих теоретичних результатів запропоновано методи ідентифікації та автентифікації віддалених користувачів, що реалізують криптографічно строгу концепцію нульових знань в алгебрі полів Галуа. Оскільки ці операції виконуються на один-два порядки швидше за мультиплікативні операції модулярної арифметики, що лежать в основі відомих методів криптографічно строгої ідентифікації, використання запропонованих методів дозволяє суттєво прискорити процес ідентифікації та автентифікації віддалених користувачів.

СПИСОК ЛІТЕРАТУРИ

1. *Schneier B.* Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed. John Wiley. NY, 1996, 758 p.
2. *Stavroulakis P.* Efficient zero—Knowledge identification based on one way Boolean transformations// IEEE. GLOBECOM Workshops (GC Wkshps). Houston, 2011, p. 275—280.
3. *Feige U., Fiat A., Shamir A.* Zero knowledge proofs of identity // Journal of Cryptology. 1988, vol. 1, № 2, p. 77—94.
4. *Мухін В.Є., Захаріудакіс Лефтеріс, Герасименко О.Ю., Козерацький М.С.* Метод ідентифікації віддалених абонентів на основі концепції «нульових знань» // Телекомунікаційні та інформаційні технології. 2017, № 1 (54), с. 37—45.
5. *Николайчук Я.М.* Коди поля Галуа: теорія та застосування. Тернопіль: ТзОВ «Терно граф». 2012, 576 с.
6. *Markovskyy O., Bardis N., Doukas N.* Fast subscriber identification based on the zero knowledge principle for multimedia content distribution // International Journal of Multimedia Intelligence and Security. 2010, vol. 1, p. 78—82.

Надійшла 03.10.17

REFERENCES

1. Schneier, B. (1996), Applied cryptography. Protocols. Algorithms and source codes in C., Ed. John Wiley, NY, USA.
2. Stavroulakis, P. (2011), “Efficient zero-knowledge identification based on one way Boolean transformations”, *IEEE of GLOBECOM Workshops*, Houston, Texas, USA, December 5-9, 2011, pp. 275-280.

3. Feige, U., Fiat, A. and Shamir, A. (1988), "Zero knowledge proofs of identity", *Journal of Cryptology*, Vol. 1, no. 2, pp. 77-94.
4. Mukhin, V.E., Zacharioudakis Leftherios, Gerasimenko, O.Yu. and Kozeratskiy, M.S. (2017), "Method of zero-knowledge identification of remote users based on the conception of "zero knowledge", *Telecommunikatsiyni ta informatsiyni tekhnologii*, Vol. 54, no. 1, pp. 37-45.
5. Nikolaychuk, Ya.M. (2012), *Kody polya Galua: teoriya ta zastosuvannya* [Galois field codes: theory and applications], TzOV Ternograf, Ternopil, Ukraine.
6. Markovskyy, O., Bardis, N. and Doukas, N. (2010), "Fast subscriber identification based on the zero knowledge principle for multimedia content distribution", *International Journal of Multimedia Intelligence and Security*, no. 1, pp. 78-82.

Received 03.10.17

O.P. Markovskiy, Zacharioudakis Leftherios, V.R. Maksymuk

GALOIS FIELDS ALGEBRA UTILIZATION FOR IMPLEMENTATION OF THE CONCEPTION OF ZERO-KNOWLEDGE UNDER IDENTIFICATION AND AUTHENTICATION OF REMOTE USERS

The new approach is proposed to implementation of theoretically strict identification and authentication of remote users in accordance with zero-knowledge conception. The proposed approach consists in the use of irreversible transformations of the Galois field algebra. This allows us to speed up the process of user identification process both under software and hardware implementation. The cyclic properties of special class Galois field exponentiation have been investigated. Based on those properties the procedures of user registration and user identification procedures have been developed. A numerical example for designed procedures is given. It is shown, both theoretically and experimentally that the proposed approach provides for acceleration of user authentication process by 1-2 orders of magnitude, via a hardware implementation.

K e y w o r d s: zero-knowledge conception, remote users identification, authentication of users, irreversible transformation on Galois fields.

МАРКОВСЬКИЙ Олександр Петрович, канд. техн. наук, доцент Національного технічного університету України «Київський політехнічний ін-т». В 1978 р. закінчив Київський політехнічний ін-т. Область наукових досліджень — захист комп'ютерних систем, даних та програм. Відновлення даних та виправлення помилок.

ЗАХАРІУДАКІС Лефтерис, ст. викладач Навчального центру імені Макарія (Нікозія, Кіпр). В 1999 г. закінчив Національний технічний університет України «Київський політехнічний ін-т». Область наукових досліджень — захист інформації в розподілених комп'ютерних системах.

МАКСИМУК Вікторія Романівна, студентка Національного технічного університету України «Київський політехнічний ін-т». Область наукових досліджень – захист інформації в розподілених комп'ютерних системах і мережах.