УДК 004.074.32

Олександр Марковський,
Вікторія Максимук

МЕТОД СТРОГОЇ АВТЕНТИФІКАЦІЇ ВІДДАЛЕНИХ АБОНЕНТІВ НА ОСНОВІ АЛГЕБРИ ПОЛІВ ГАЛУА

METHOD FOR STRONG REMOTE USERS BASED ON GALOIS FIELDS ALGEBRA

Представлений новий метод реалізації теоретичної строгої перевірки віддалених користувачів на основі концепції «нульового знання». Запропонований підхід полягає в застосуванні математичної операції експоненціювання на полях Галуа замість модульної експоненти. Це дозволяє прискорити процес ідентифікації для апаратної реалізації. Технологія математичних перетворень, що надаються запропонованим методом, викладена чітко. Наведено числовий приклад для розроблених процедур реєстрації користувача.

Ключові слова: концепція «нульових знань», ідентифікація віддалених користувачів, автентифікація користувачів, незворотні перетворення на полях Галуа.

Бібл.: 5.

The new method for implementation of theoretical strong autentification of remote users based on zero-knowledge conception is presented. The proposed method consist of using of mathematical operation of exponentiation on Galois fields instead of modular exponentiation. It allows to speed up of identification process for hardware implementation. The technology of mathematical transformations whose are provided by proposed method are set forth clearly. A numerical example for designed procedures of user registration.

Key words: zero-knowledge conception, remote users identification, users authentication, irreversible transformation in Galois fields.

Bibl.: 5.

Актуальність теми дослідження. 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, 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 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 автентифікації віддалених користувачів. Разом з тим, поява хмарних технологій має наслідком значне зростання кількості користувачів, для якісного обслуговування яких потрібно радикально прискори-

ти процедури контролю їх доступу до інформаційних та обчислювальних ресурсів.

Таким чином, задача підвищення ефективності засобів автентифікації віддалених користувачів є актуальною та важливою з огляду особливостей сучасного етапу розвитку інформаційних технологій.

Постановка проблеми. В сучасних умовах і у найближчій перспективі потрібний для практики рівень надійності автентифікації може бути забезпечений лише методами, що спираються на концепцію нульових знань [2]. Ця концепція передбачає наступні елементи:

- Пароль користувача змінюється при кожному зверненні до системи.
- Користувач має спеціальний механізм генерації правильних паролей.
- Система не може генерувати правильних паролей, але має механізм перевірки їх правильності.

Для побудови ідентифікації на основі концепції нульових знань потрібне використання спеціальних криптографічних незворотних та неоднозначних перетворень. Ефективність ідентифікації визначається рівнем не оберненості перетворення та об'ємом часових ресурсів на його реалізацію. Проблема побудови ефективної схеми ідентифікації зводиться до найбільш вдалого розв'язання компромісу між вказаними чинниками.

Аналіз основних досліджень і публікацій. Найбільш відомими методами, які реалізують цю концепцію є FFSIS(Feige Fiat Shamir Identification Scheme)[3], методи Шнора (Schnorr) та Гіллоу—Квіскатера (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 розрядності чисел становить 2048 або 4096, швидкість ідентифікації обмежуються значною обчислювальною складністю цих операцій і, відповідно, виникає необхідність в її зменшенні.

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

Виділення недосліджених частин загальної проблеми. Аналіз існуючих систем строгої ідентифікації показав, що основним недоліком існуючих протоколів та механізмів є значна обчислювальна складність. В сучасних умовах зростання розрядності цей недолік має наслідком порушення часових рамок протоколів мережевого захисту. Тому важливим завданням є розробка нових незворотних перетворень обчислювальна реалізація яких потребує менше часу. Одним з найбільш перспективних напрямків є перехід до альтернативних алгебраїчних базисів.

Постановка завдання. Метою дослідження є зменшення обчислювальної складності процесу криптографічно строгої автентифікації на основі концепції нульових знань при забезпеченні високого рівня захищеності за рахунок застосування альтернативного алгебраїчного базису – скінченних полів Галуа.

Теоретичне підґрунтя. Аналогічно тому, як у традиційній алгебрі в якості базової операції широкого кола механізмів криптографічного захисту використовується модулярне експоненціювання $A^E \bmod M$, в алгебрі скінчених полів Галуа для криптографічних застосувань в якості базової застосовується експоненціювання $A^E \operatorname{rem} M$ полях [4].

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

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

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

Якщо $g(x)$ – простий поліном ступеню d, то для будь-якого $u(x)$,що є елементом поля GF(2^d) і якому співвідноситься d-розрядне двійкове число u, таке, що 0<u h, де h=2^d-1 виконується [4] :

$$u\ |^{h+1}\ rem\ g = u \quad (2)$$

Якщо утворюючий поліном $M(x)$ ступеню r являє собою добуток двох простих поліномів $p(x)$ ступеню v і $g(x)$ ступеню d : $M(x)=p(x)g(x)$, $r = v+d$, причому поліному $M(x)$ співвідноситься двійкове число m то для будь-якого $u(x)$, що належить полю GF(2^v) і з яким співвідноситься число u, u $h=2^d$-1 справедливо:

$$(u \otimes p)\ |^{h+1}\ rem\ m = u \otimes p \quad (3)$$

Наприклад, якщо $p(x) = x^3+x^2+1$ простий поліном ступеню 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 ступеню d= 5, якому відповідає число g= 59, для якого $h = 2^5$-1 = 31, то добуток цих поліномів має вигляд $M(x) = p(x)\ g(x) = x^8 + x^3 + x^2 + x + 1$, і співвідноситься з числом m=271. Якщо вибрати число u таким чином, що 0<u h-1, зокрема, u = 28, то up = 140. Тоді $(up)|^{h+1}$ rem m = $(2813)|^{32}$ rem 271 = 140.

Аналогічно, для будь-якого поліному $w(x)$, що належить полюGF(2^d) та співвідноситься з числом w, так, що wl=2^v-1 справедливо:

$$(w \otimes g)\ |^{l+1}\ rem\ m = w \otimes g \quad (4)$$

Якщо в рамках наведеного прикладу вибрати довільне w менше за l: 0 <w<l, наприклад, w= 5, то добуток wg = 559 = 215. Відповідно, $(wg)^{l+1}$ rem m = $(5\ 59)^8$ rem 271 = 215, тобто дорівнює згідно (3) w g. Доведення формул (3) і (4) виконано в роботі [5]

Таким чином, знання однією зі сторін процесу ідентифікації періоду повторення експоненціювання дозволяє будувати ефективні алгоритми ідентифікації в рамках криптографічно строгої концепції “нульових знань”.

Метод строгої автентифікації абонентів з використанням алгебри полів Галуа. Запропонований в попередньому розділі 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, що система взаємодіє з авторизованим користувачем, але надає користувачеві механізми, які дозволяють впевнитися в тому, що він взаємодіє дійсно з системою.

Пропонована процедура реєстрації передбачає наступну послідовність дій:

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

2)Користувач довільним чином вибирає пару простих поліномів $p(x)$та $g(x)$з різними степенями: $p(x)= x^v + p_{v-1}\cdot x^v + \ldots + p_1\cdot x + p_0$ степені v та $g(x)= x^d +$

$+ g_{d-1} \cdot x^{d-1} + \ldots + g_1 \cdot x + g_0$ степені d, де $p_0, p_1, \ldots, p_{v-1}$ {0,1}, $g_0, g_1, \ldots, g_{d-1}$ {0,1}, причому $d>v$.

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

4) Користувач вибирає випадкове число : 0<< 2^d та обчислює другу компоненту відкритого ключа користувача у вигляді: $= p$ rem m.

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

6) Всі три компоненти m , та ключа користувача шифруються відкритим закриваючим ключем $К_с$ і відсилаються системі.

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

Пропонована процедура реєстрації може бути ілюстрована наступним прикладом. У відповідності з п.2 Користувач вибирає простий поліном ступеню 3 (v=3) $p(x)= x^3 + x^2 + 1$, яке співвідноситься з числом p=11, та простий поліном степені 5 (d=5) $g(x) = x^5 + x^4 + x^3 + x +1$, якому співвідноситься число g = 59. Згідно з п.2 користувач формує утворюючий поліном $M(x)$ як поліноміальний добуток вибраних простих поліномів: $M(x) = p(x)g(x) = x^8 + x^7 + x^4 + x^2 + 1$, який співвідноситься з числом m = 405. Згідно з п.4 процедури реєстрації користувач випадковим чином обирає число = 18 та обчислює другу компоненту ключа: $= p$ rem $m = 11^{18}$ rem 405 = 49. Згідно п.5 запропонованої процедури користувач вибирає довільне менше $2^{d+v}-2^{d+1} = 192$. Нехай, вибране значення дорівнює 18, тобто =18. Користувач обчислює значення $= 2^{d+v}-2^d-2^v + 1 -$ = 218 – 18 = 200.

Трійка компонентів ключа користувача < 405, 49, 18 > шифрується відкритим ключем $К_с$ 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 ключа користувача обчислює значення $= r$ rem m. Коди r та відсилає користувачеві.

3) Користувач приймає від системи код r та . Для перевірки того, що він працює дійсно з системою, обчислює $= r$ rem m. Якщо $= r$, тобто поліноміальний добуток обчисленого на отриманий код дорівнює отриманому від системи числу r, то користувач впевнюється, що сторона, яка надіслала йому коди r та дійсно знає компоненти його ключа m та , тобто є системою.

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

5) Користувач обчислює сеансовий пароль у вигляді $= p|$ rem m після чогошифрує за допомогою відкритого ключа $К_с$ отриманий код та надсилає його системі.

6) Система, отримавши зашифрований сеансовий пароль , розшифровує його своїм секретним відкриваючим ключем $К_о$ та обчислює $y = |^r$ rem M.

Отримане значення у порівнюється з другою компонентною відкритого ключа цього користувача: якщо ці коди співпадають, тобто $y =$, 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 п.2 процедури, у відповідь на звернення користувача, система випадковим чином вибирає число $r = 28$ і обчислює $= r \text{ rem } m = 28^{18} \text{ rem } 405 = 38$, після чого пересилає його користувачеві $r=28$ та $=38$.

Користувач приймає від системи надіслані йому коди $r = 28$ та $=38$. Для того, щоб впевнитися, що сторона, яка надіслала йому ці коди дійсно знає його ключ, тобто є системою користувач згідно п.3 обчислює $= r \text{ rem } m = 28^{200} \text{ rem } 405 = 117$. Далі користувач обчислює поліноміальний добуток $= 11738 = 28$. 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 з п.4 описаної вище процедури, користувач віднаходить таке w, для якого виконується умова: $28w \bmod 31 = 18$. Ця умова виконується для $w= 25$. Згідно з п.5 користувач обчислює сеансовий пароль у вигляді $= p| \text{ rem } m = 11|^{25} \text{ rem } 405 = 245$. Цей сеансовий пароль користувач посилає системі. Згідно з п. 6, система отримавши зашифрований сеансовий пароль , розшифровує його своїм секретним відкриваючим ключем K_o та обчислює $y = |^r \text{ rem } m = 245|^{28} \text{ rem } 405 = 49$. Це значення порівнюється з другою компонентою ключа користувача. Оскільки обчислене значення $y = 49$ співпадає зі значенням другої компоненти реєстраційного ключа цього конкретного користувача = 49, то система успішно його ідентифікує.

Оцінка ефективності. 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 поліному $M(x)$ поля Галуа; з позицій зловмисника, що має доступ до даних, що зберігаються в системі, і зокрема коду $M(x)$. $p(x)$та $g(x)$

Очевидно, що для того, щоб виконати успішний підбір коректного паролю користувача потрібно знати простий поліном $g(x)$, а також степінь v іншого простого поліному $p(x)$. Найдоцільніша технологія підбору компоненти паролю $p(x)$ для стороннього зловмисника полягає в перехопленні коду $q(x) = k(x)p(x)$ та розкладенні його на співмножники. Важливим моментом при цьому є те, що у зловмисника практично відсутній критерій коректності розкладення. Ще одна особливість задачі розкладання коду $q(x)$ на співмножники полягає в тому, що один з них 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 степінь поліному становить сотні і, відповідно, задача перебору простих поліномів далеко виходить 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 поліному $M(x)$ на два простих множника $p(x)$ та $g(x)$ з різними ступенями. Як уже зазначалося, вище вирішення такої задачі шляхом перебору для реальних степенів поліномів виходить далеко на межі технічних можливостей сучасних комп'ютерних систем.

Висновки. На основі отриманих теоретичних результатів запропоновано методи ідентифікації та автентифікації віддалених користувачі, 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 автентифікації відлених користувачів.

Список літератури

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

2. Feige U. Zero knowledge proofs of identity / Feige U.,Fiat A.,Shamir A.// Journal of Cryptology.- v.1.- №.2.- 1988, pp.77-94.

3. Markovskyy O. Fast subscriber identification based on the zero knowledge principle for multimedia content distribution/ O. Markovskyy, N. Bardis, N. Doukas // International Journal of Multimedia Intelligence and Security 2010 - Vol. 1,- pp.78-82.

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. Марковський О.П. Використання алгебри полів Галуа для реалізації концепції «нульових знань» при ідентифікації та автентифікації віддалених користувачів /О.П. Марковський, Захаріудакіс Лефтеріс, В.Р. Максимук // Электронное моделирование.-том 39.-№6.-2017.-С.33-46.

ДОВІДКА ПРО АВТОРІВ

Марковський Олександр Петрович – кандидат технічних наук, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Oleksandr Markovskyi – Associate Professor, PhD, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Максимук Вікторія Романівна – студентка, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Viktoriia Maksymuk – student, Department of Computer Engineering, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

Марковський О. П.,
Максимук В. Р.

METHOD FOR STRONG REMOTE USERS BASED ON GALOIS FIELDS ALGEBRA

Acute problem. A particularly acute problem, is the problem of fast algorithms for identification architectures based on the concept of "zero – knowledge" in mobile devices and embedded microcontrollers, with limited energy consumption possibilities, that are commonly end user devices. In this context, the problem of acceleration of user identification based on zero knowledge is imminent and has a wide range of practical applications.

Target setting. FFSIS is a relatively simple and at the same time sufficiently effective scheme for the identification of the subscribers of multi-user systems, on the basis of which a number of more practical to use modified algorithms have been proposed. In the attempts of using this scheme in practice, the main disadvantage of FFSIS is the need for a large number of data exchanges during the user identification process, which noticeably loads the communication channels used. Other existing identification schemes, which implement the zero knowledge concept, require a substantially smaller volume of data transfers, but the procedures provided by them involve large computational complexity, since instead of the operation of squaring, they use the modular exponential operation.

Actual scientific researches and issues analysis. In literature identification methods, which satisfy the first three of the given requirements are classified as "strict", in contrast the remaining schemes that are classified as "weak". In the class of the weak schemes belong, for example, the procedure of identification which used in the UNIX operating system. This procedure involves the storage in the system of only the hash value of the passwords of users, that, with the use of the one way hash functions, excludes the possibility of the reproduction of password of the system; however, passwords themselves do not change, which makes it sufficient simple to intercept them. The class of strict procedures is principally composed by methods of identification that are based the concept "zero knowledge". The most commonly known of these methods are the FFSIS (Feige Fiat Shamir Identification Scheme) [3], Guillou- Quisquater [4] and Schnorr identification schemes [5].

Uninvestigated parts of general matters defining. The main disadvantage of known identification schems consist of that schemes demand a significantly smaller volume of data exchanges compared to the FFSIS, but their implementation involves a significantly large computational volume, as the squaring operation has been replaced by the modular exponentiation. The FFSIS is considered more economic in terms of the volume of the calculations involved, but its application demands several cycles of information exchange.

The research objective. The purpose of this research is the development of a modified architecture for zero knowledge user identification, which involves significantly smaller computational complexity and increases the speed of identification with software and hardware implementations.

The statement of basic materials. The proposed method, contrary to existing techniques uses a single session for the registration between the user and the system.

Conclusions. In this paper, zero – knowledge user authentication using non – reversible transformation in Galois fields was investigated and a scheme for such authentication was proposed. For this purpose a theoretical study was conducted of the properties of specific cycles that appear during exponentiation in the context of special cases of Galois fields. The theoretical results enabled the development of procedures for the registration and authentication of remote users. It was theoretically determined that the level of security attained does not differ from existing zero knowledge systems. The principal advantage of the proposed method is the possibility of achieving significantly higher rates of authentication. This increased rate is of vital importance in current applications with ever growing numbers of system users and the necessity for remote information processing. Maximum effectiveness of the proposed method is attained by implementation in hardware.

Key words: zero-knowledge conception, remote users identification, users authentication, irreversible transformation in Galois fields.