бора проектного решения для развертывания сети LTE с учетом потребностей защиты информации. Рассмотрены основные требования пользователей к сетям нового поколения, проанализированы каким образом они влияют на выбор оборудования для построения сети. Предложено и обосновано описание матрицы выбора решения, на базе которой в конечном итоге происходит выбор проектного решения, согласно требованиям пользователей.

Ключевые слова: сотовые сети связи, базовая станция, LTE, матрица выбора решения, проект, требования пользователей, архитектура решения.

METHODOLOGY FOR THE SELECTION OF DESIGN SOLUTIONS FOR THE DEPLOYMENT OF SECURE LTE NETWORK

To maintain high-speed applications, the use of new services , support continuous mobile access to the Internet telecom operators need to develop plans for the implementation of new technologies and update existing business communications with the general trend of scientific and technological innovation and development. Strong demand in the market of communication services is offset by the presence of even greater demand. Often the customer telecommunication solutions to the huge amount offered him a variety of services for which prices vary by orders of magnitude is unable to make the right choice. It is based on this position you must offer a technique whose purpose will be to harmonize consumer requests to the communication system based on packet data through the channels of modern mobile communication systems fourth generation. The paper presents a step by step methodology for selecting design solution for LTE network deployment, taking into account the need to protect information. The basic user requirements to next generation networks and analyzes how they affect the selection of equipment for the construction of the network. A reasonable description and selection decision matrix, based on which the final result is the choice of design solution, according to the requirements of users.

Keywords: cellular networks, base station, LTE, choice of matrix solution, project, user requirements, architecture decisions.

Одарченко Роман Сергійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.
E-mail: odarchenko.r.s@mail.ru
Одарченко Роман Сергеевич, кандидат технических наук, доцент кафедры телекоммуникационных систем института аэронавигации Национального авиационного университета.
Roman Odarchenko, Ph.D., Associate Professor of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

Ткаченко Вадим Валерійович, аспірант кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.
E-mail: vtkachenko@mts.com.ua
Ткаченко Вадим Валерьевич, аспирант кафедры телекоммуникационных систем института аэронавигации Национального авиационного университета
Vadim Tkachenko, a graduate student of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

Конахович Георгій Филимонович, доктор технічних наук, професор, завідувач кафедри телекомунікаційних систем інституту аеронавігації Національного авіаційного університету.
E-mail: tks@nau.edu.ua
Конахович Георгий Филимонович, доктор технических наук, профессор, заведующий кафедрой телекоммуникационных систем института аэронавигации Национального авиационного университета.
George Konahovich, prof., Head of Telecommunication Systems department of Institute of Air Navigation of the National Aviation University.

УДК 681.3.067

АЛГЕБРАЇЧНІ МОДЕЛІ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ СИСТЕМ

Юрій Яремчук

Моделювання криптографічних методів на рівні алгебраїчних структур дає можливість глибше зрозуміти принципи їх побудови, особливості функціонування, дослідити їх властивості. Існуючи на сьогодні алгебраїчні моделі асиметричних криптографічних систем не забезпечують в повній мірі можливості їх використання. В роботі розглянуто алгебраїчну модель відкритого розподілу секретних ключів, а також запропоновано алгебраїчні моделі асиметричного шифрування, автентифікації сторін взаємодії та цифрового підписування як багатоосновні універсальні алгебри. На основі представлених алгебр розглянуто моделі існуючих криптосистем, а також запропоновано моделі розподілу секретних

ключів та асиметричного шифрування з використанням математичного апарату рекурентних U_k *– та* V_k *–послідовностей. Запропоновано різні варіанти моделей автентифікації сторін взаємодії та цифрового підписування з використанням математичного апарату рекурентних* V_k *–послідовностей, які в різних випадках забезпечують спрощення обчислення та підвищення криптографічної стійкості у порівняні з відомими аналогами.*

Ключові слова: *криптографія, алгебраїчні моделі, розподіл ключів, асиметричне шифрування, автентифікація сторін взаємодії, цифрове підписування.*

Вступ. Моделювання методів та алгоритмів криптографічних перетворень інформації за допомогою алгебраїчних структур дає можливість більш глибоко зрозуміти принципи їх побудови та функціонування і дозволяє на абстрактному рівні вирішувати різного роду теоретичні задачі аналізу та синтезу методів і алгоритмів таких перетворень. По суті вперше загальна модель криптографічної системи була запропонована К. Шенноном [1].

Для моделювання на абстрактному рівні криптографічних методів та систем можна використовувати універсальні алгебри та системи [2, 3]. В [4–7] для побудови такого роду моделей пропонується використовувати алгебраїчні структури багатоосновних універсальних алгебр. В [4] представлено модель так званої public key– або pk – алгебри для побудови системи відкритого розподілу секретних ключів, а в [6] представлено алгебраїчні моделі криптосистем асиметричного шифрування та цифрового підписування як багатоосновні універсальні алгебри. Однак, ці алгебраїчні моделі забезпечують можливість представлення на абстрактному рівні лише певної частини асиметричних криптосистем. Крім того, вони не забезпечують представлення криптосистем автентифікації сторін взаємодії, а також не враховують можливість представлення асиметричних криптосистем на основі математичного апарату рекурентних послідовностей.

Це особливо актуально, оскільки запропонований в [8-12] математичний апарат рекурентних V_k – та U_k –послідовностей дозволяє будувати асиметричні криптографічні методи різного призначення, причому так, що вони можуть за різних умов забезпечувати спрощення обчислень та підвищення криптографічної стійкості у порівняні з відомими аналогами. Тому розробка моделей асиметричних криптосистем на основі рекурентних V_k – та U_k –послідовностей дасть можливість глибше дослідити їх властивості.

V_k – та U_k –послідовності [8] являють собою рекурентні послідовності, в яких коефіцієнти рекурентного співвідношення пов'язані з початковими елементами послідовності.

V_k –послідовність [8] складається з V_k^+ – та V_k^- –послідовності.

V_k^+ –послідовністю називається послідовність чисел, що обчислюються за формулою

$$v_{n,k} = g_k v_{n-1,k} + g_1 v_{n-k,k} \qquad (1)$$

для початкових значень $v_{0,k} = 1$, $v_{1,k} = g_2$ для $k = 2$; $v_{0,k} = v_{1,k} = \ldots = v_{k-3,k} = 0$, $v_{k-2,k} = 1$, $v_{k-1,k} = g_k$ для $k > 2$; де g_1, g_k – цілі числа; n і k – цілі додатні.

Обчислення елементів цієї послідовності для спадних n, починаючи з деякого значення $n = l$, буде здійснюватись таким чином

$$v_{n,k} = \frac{v_{n+k,k} - g_k \cdot v_{n+k-1,k}}{g_1}. \qquad (2)$$

V_k^- –послідовністю називається послідовність чисел, що обчислюються за формулою (2) для n – від'ємних при початкових значеннях $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$ для $k = 2$; $v_{-1,k} = 0$, $v_{-2,k} = g_1^{-1}$, $v_{-3,k} = v_{-4,k} = \ldots = v_{-k,k} = 0$ для $k > 2$.

В [8, 9] представлено такі аналітичні залежності обчислення елементів V_k –послідовності з адитивною зміною індексу для будь-яких цілих додатних n, m та k

$$v_{n+m,k} = v_{m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (3)$$

$$v_{n-m,k} = v_{-m+(k-2),k} \cdot v_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{-m+(k-2)-i,k} \cdot v_{n-k+i,k}. \qquad (4)$$

$$v_{-n+m,k} = v_{m+(k-2),k} \cdot v_{-n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot v_{-n-k+i,k}. \qquad (5)$$

U_k –послідовністю [8] називається послідовність чисел, що обчислюються за формулою

$$u_{n,k} = g_k u_{n-1,k} + g_1 u_{n-k,k} \qquad (6)$$

для початкових значень $u_{0,k} = g_1$, $u_{1,k} = g_2$, $u_{2,k} = g_3$, ... $u_{k-1,k} = g_k$; де g_1, g_2, g_3, ..., g_k – цілі числа; n і k – цілі додатні числа.

Для будь-яких цілих додатних n, m та k отримано таку залежність [8]

$$u_{n+m,k} = v_{m+(k-2),k} \cdot u_{n,k} + g_1 \cdot \sum_{i=1}^{k-1} v_{m+(k-2)-i,k} \cdot u_{n-k+i,k} \,. \qquad (7)$$

Для будь-яких цілих додатних n та k, таких що $n \geq k$, отримано залежність [8]

$$u_{n,k} = g_k \cdot v_{n-1,k} + g_1 \cdot \sum_{i=1}^{k-1} g_i \cdot v_{n-i-1,k} \,. \qquad (8)$$

Постановка задач досліджень. Використовуючи математичний апарат універсальних алгебр та систем, зокрема багатоосновної pk–алгебри, розробити алгебраїчні моделі асиметричних криптографічних систем розподілу секретних ключів, шифрування інформації, автентифікації сторін взаємодії та цифрового підписування, розглянувши при цьому можливість розробки моделей асиметричних криптосистем на основі рекурентних V_k – та U_k –послідовностей.

Алгебраїчні моделі відкритого розподілу секретних ключів. Модель так званої public key– або pk–алгебри [4] являє собою узагальнення відомих раніше систем відкритого розподілу секретних ключів, вона представляється у вигляді алгебраїчної конструкції з 5-ти скінчених непустих множин та 4-х відображень, пов'язаних однією тотожністю: K_1 та K_2 – множини секретних ключів першого та другого користувачів відповідно; D_1 та D_2 – множини відкритої ключової інформації першого та другого користувачів відповідно; S – множина спільних ключів; ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$ – сюр'єктивні відображення; ψ_1: $K_1 \times D_2 \to S$, ψ_2: $K_2 \times D_1 \to S$ – сюр'єктивні відображення; причому для усіх $k_1 \in K_1$, $k_2 \in K_2$ виконується рівняння

$$\psi_1\left(k_1, \phi_2(k_2)\right) = \psi_2\left(k_2, \phi_1(k_1)\right). \qquad (9)$$

Описану алгебраїчну конструкцію відкритого розподілу секретних ключів названо [4] pk–алгеброю (public key)

$$\mathrm{A} = \left(K_1, K_2, D_1, D_2, S, \phi_1, \phi_2, \psi_1, \psi_2\right). \qquad (10)$$

pk–алгебра A вважається загальнодоступною. Два користувача, обмінюючись інформацією відкритим каналом зв'язку виробляють спільний ключ $s \in S$ таким чином. Кожен з них обирає тільки йому відомий елемент з множини секретних ключів $k_1 \in K_1$, $k_2 \in K_2$, та обчислює $\phi_1(k_1) \in D_1$ і $\phi_2(k_2) \in D_2$. Після цього вони обмінюються відкритою інформацією: перший надсилає другому елемент $\phi_1(k_1)$, а другий першому – $\phi_2(k_2)$. На завершення вони обчислюють спільний ключ $s \in S$: перший користувач обчислює його у вигляді $\psi_1\left(k_1, \phi_2(k_2)\right)$, а другий – у вигляді $\psi_2\left(k_2, \phi_1(k_1)\right)$. Виходячи з тотожності (9), обчислені першим та другим користувачем елементи будуть збігатись.

В [4] розглянуто вимоги та особливості безпеки представленої системи вироблення спільного ключа на основі pk–алгебри, яка базується на тому, що зловмисник має усю інформацію, що надсилають користувачі один одному, має певні (обмежені) обчислювальні ресурси, але не може відновити вироблений користувачами спільний ключ $s \in S$. Тобто безпека системи визначається складністю вирішення математичної задачі: за відомими значеннями $d_1 \in \phi_1(K_1) = D_1$, $d_2 \in \phi_2(K_2) = D_2$, не знаючи $k_1 \in K_1$, $k_2 \in K_2$, знайти невідомий елемент $s = \psi_1\left(k_1, \phi_2(k_2)\right) = \psi_2\left(k_2, \phi_1(k_1)\right)$. Дана задача зводиться до іншої математичної задачі: з невідомого елементу $d_1 \in \phi_1(K_1)$ (або $d_2 \in \phi_2(K_2)$) знайти хоча б одне k_1 (або k_2) з рівняння $\phi_1(k_1) = d_1$ (або $\phi_2(k_2) = d_2$). Таким чином, вимоги безпеки означають, що складність вирішення цих математичних задач в даній pk–алгебрі A є достатньо високою.

Відзначимо, що знаходження явного вигляду відображень ψ_1, ψ_2 та ϕ_1, ϕ_2 є дуже нетривіальною математичною задачею: для чотирьох функцій маємо всього одне функціональне співвідношення (9). Тому на сьогодні існують лише лічені конкретні приклади цих функцій.

Прикладом розглянутої моделі розподілу секретних ключів на основі pk–алгебри A є криптографічна система Діффі-Хеллмана [13].

Приклад 1. (система розподілу секретних ключів Діффі-Хеллмана)

Нехай p – просте число, $GF(p) = \{0,1,...,p-1\}$ – просте поле Галуа, g – породжуючий елемент $GF(p)^*$, $1 < g < p-1$. Покладемо $K_1 = K_2 = D_1 = D_2 = S = GF(p)^*$.

Визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, ψ_1: $K_1 \times D_2 \to S$ та ψ_2: $K_2 \times D_1 \to S$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = g^{k_1} \bmod p\,,\ \phi_2(k_2) = g^{k_2} \bmod p\,, \qquad (11)$$

$$\psi_1\left(k_1, \phi_2(k_2)\right) = \left(g^{k_2}\right)^{k_1} \bmod p\,,$$

$$\psi_2\left(k_2, \phi_1(k_1)\right) = \left(g^{k_1}\right)^{k_2} \bmod p\,. \qquad (12)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\mathrm{A}_{DH} \overset{def}{=} \left(K_1, K_2, D_1, D_2, S, \phi_1, \phi_2, \psi_1, \psi_2\right)$,

яку назвемо криптосистемою розподілу секретних ключів Діффі-Хеллмана, виконується рівняння (9).

Стійкість криптосистеми A_{DH} визначається складністю обчислення k_1 з $g^{k_1} \bmod p$ (або k_2 з $g^{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Запропонуємо тепер моделі розподілу секретних ключів на основі pk–алгебри A з використанням математичного апарату рекурентних послідовностей.

Приклад 2. (система розподілу секретних ключів на основі рекурентних U_k–послідовностей)

Нехай p – просте число. Покладемо $K_1 = K_2 = D_1 = D_2 = S = GF(p)$, де $GF(p) = \{0,1,...,p-1\}$ – просте поле Галуа.

На основі математичного апарату рекурентних U_k–послідовностей визначимо сюр'єктивні відображення $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\psi_1 : K_1 \times D_2 \to S$ та $\psi_2 : K_2 \times D_1 \to S$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = u_{k_1} \bmod p,\ \phi_2(k_2) = u_{k_2} \bmod p, \qquad (13)$$

$$\psi_1\left(k_1, \phi_2(k_2)\right) = u_{k_2+k_1} \bmod p,$$

$$\psi_2\left(k_2, \phi_1(k_1)\right) = u_{k_1+k_2} \bmod p. \qquad (14)$$

Багатоосновну алгебру $A_U \overset{def}{=} (K_1, K_2, D_1, D_2, S, \phi_1, \phi_2, \psi_1, \psi_2)$ назвемо криптосистемою розподілу секретних ключів на основі U_k–послідовностей. Рівняння (9) буде виконуватись для U_k–послідовностей, оскільки з аналітичної залежності (7) видно, що $u_{n+m,k} = u_{m+n,k}$ для будь-яких цілих додатних n, m та k, і ці значення елементів можуть бути обчислені згідно залежності (7).

Стійкість криптосистеми A_U визначається складністю обчислення k_1 з $u_{k_1} \bmod p$ (або k_2 з $u_{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу рекурентної послідовності, обчисленого за модулем для великого значення індексу. В [12] показано, що ця задача є не менш складною, ніж задача обчислення дискретного логарифму в полі $GF(p)$.

Приклад 3. (система розподілу секретних ключів на основі рекурентних V_k–послідовностей)

Якщо p – просте число, то покладемо $K_1 = K_2 = D_1 = D_2 = S = GF(p)$.

На основі математичного апарату рекурентних V_k–послідовностей визначимо сюр'єктивні відображення $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\psi_1 : K_1 \times D_2 \to S$ та $\psi_2 : K_2 \times D_1 \to S$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = v_{k_1} \bmod p,\ \phi_2(k_2) = v_{k_2} \bmod p, \qquad (15)$$

$$\psi_1\left(k_1, \phi_2(k_2)\right) = v_{k_2 \cdot k_1} \bmod p,$$

$$\psi_2\left(k_2, \phi_1(k_1)\right) = v_{k_1 \cdot k_2} \bmod p. \qquad (16)$$

Назвемо алгебру $A_V \overset{def}{=} (K_1, K_2, D_1, D_2, S, \phi_1, \phi_2, \psi_1, \psi_2)$ криптосистемою розподілу секретних ключів на основі V_k–послідовностей. Справедливість рівняння (9) для V_k–послідовностей буде виконуватись, оскільки $v_{n \cdot m,k} = v_{m \cdot n,k}$ і ці значення елементів можуть бути обчислені за модулем p за алгоритмом прискореного обчислення елементу V_k–послідовності з мультиплікативною зміною індексу [11] на основі аналітичної залежності (3) обчислення елементів $v_{n+m,k}$ для будь-яких цілих додатних n, m та k.

Стійкість криптосистеми A_V визначається складністю обчислення k_1 з $v_{k_1} \bmod p$ (або k_2 з $v_{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу рекурентної послідовності, обчисленого за модулем для великого значення індексу. В [12] показано, що ця задача є не менш складною, ніж задача обчислення дискретного логарифму в полі $GF(p)$.

Алгебраїчні моделі асиметричного шифрування інформації. По аналогії з pk–алгеброю, використаємо тепер багатоосновну універсальну алгебру для побудови моделі асиметричного шифрування інформації.

Модель асиметричного шифрування пропонується представити у вигляді алгебраїчної конструкції з 6-ти скінчених непустих множин та 4-х відображень, пов'язаних однією тотожністю: X – множина відкритих повідомлень; S – множина зашифрованих повідомлень; K_1 – множина секретних ключів одержувача зашифрованих повідомлень; D_1 – множина відкритої ключової інформації одержувача; K_2 – множина сеансових секретних ключів відправника повідомлень; D_2 – множина відкритої сеансової ключової інформації відправника; $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$ – сюр'єктивні відображення; $\psi_1 : X \times D_1 \times K_2 \to S$,

$\psi_2 : S \times D_2 \times K_1 \to X$ – сюр'єктивні відображення; причому для усіх $x \in X$, $k_1 \in K_1$, $k_2 \in K_2$ виконується рівняння

$$x = \psi_2\left(\psi_1\left(x, \phi_1(k_1), k_2\right), \phi_2(k_2), k_1\right). \qquad (17)$$

Представлена алгебраїчна конструкція асиметричного шифрування інформації являє собою багатоосновну універсальну алгебру

$$\Omega = \left(X, S, K_1, K_2, D_1, D_2, \phi_1, \phi_2, \psi_1, \psi_2\right). \qquad (18)$$

Алгебра Ω вважається загальнодоступною. Шифрування інформації з відкритим ключем відбувається таким чином. Одержувач повідомлень, або центр довіри, вибирає секретний ключ $k_1 \in K_1$ та обчислює на його основі відкритий ключ $d_1 = \phi_1(k_1) \in D_1$, який шляхом відкритого публікування передається відправнику. Коли відправник хоче зашифрувати повідомлення і передати його одержувачу, він обирає сеансовий секретний ключ $k_2 \in K_2$, обчислює відкриту ключову інформацію $d_2 = \phi_2(k_2) \in D_2$, зашифровує відкрите повідомлення $x \in X$ шляхом обчислення $s = \psi_1\left(x, d_1, k_2\right) \in S$ та передає одержувачу зашифроване повідомлення $s \in S$ разом з відкритою ключовою інформацією $d_2 \in D_2$. Одержувач, отримавши цю інформацію, здійснює дешифрування зашифрованого повідомлення шляхом обчислення $x = \psi_2\left(s, d_2, k_1\right) \in X$, отримуючи таким чином відкрите повідомлення $x \in X$. Виходячи з тотожності (17), в результаті дешифрування зашифрованого відкритого повідомлення маємо отримати це ж саме відкрите повідомлення.

Відзначимо також, що, як і для моделі розподілу секретних ключів, знаходження явного вигляду відображень ψ_1, ψ_2 та ϕ_1, ϕ_2 є дуже нетривіальною математичною задачею: для чотирьох функцій маємо всього одне функціональне співвідношення (17). Тому на сьогодні існують лише декілька конкретних прикладів цих функцій.

Прикладом представленої моделі асиметричного шифрування інформації на основі алгебри Ω є криптографічна система Ель-Гамаля [14].

Приклад 4. (система асиметричного шифрування Ель-Гамаля)

Нехай p – просте число, $GF(p) = \{0,1,..., p-1\}$ – просте поле Галуа, g – породжуючий елемент $GF(p)^*$, $1 < g < p-1$. Покладемо $X = S = GF(p)$, $K_1 = K_2 = D_1 = D_2 = GF(p)^*$.

Визначимо сюр'єктивні відображення $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\psi_1 : X \times D_1 \times K_2 \to S$ та $\psi_2 : S \times D_2 \times K_1 \to X$ для усіх $x \in X$, $s \in S$, $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = g^{k_1} \bmod p,\ \phi_2(k_2) = g^{k_2} \bmod p, \qquad (19)$$

$$\psi_1\left(x, \phi_1(k_1), k_2\right) = x \cdot \left(g^{k_1}\right)^{k_2} \bmod p = s,$$

$$\psi_2\left(s, \phi_2(k_2), k_1\right) = s \cdot \left(g^{k_2}\right)^{-k_1} \bmod p = x. \qquad (20)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\Omega_{EG} \overset{def}{=} \left(X, S, K_1, K_2, D_1, D_2, \phi_1, \phi_2, \psi_1, \psi_2\right)$, яку назвемо криптосистемою асиметричного шифрування Ель-Гамаля, виконується рівняння (17).

Стійкість криптосистеми Ω_{EG} визначається складністю обчислення k_1 з $g^{k_1} \bmod p$ (або k_2 з $g^{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Запропонуємо тепер моделі асиметричного шифрування інформації на основі алгебри Ω з використанням математичного апарату рекурентних послідовностей.

Приклад 5. (система асиметричного шифрування на основі рекурентних U_k –послідовностей)

Нехай p – просте число. Покладемо $K_1 = K_2 = D_1 = D_2 = X = S = GF(p)$, де $GF(p) = \{0,1,..., p-1\}$ – просте поле Галуа.

На основі математичного апарату рекурентних U_k –послідовностей визначимо сюр'єктивні відображення $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\psi_1 : X \times D_1 \times K_2 \to S$ та $\psi_2 : S \times D_2 \times K_1 \to X$ для усіх $x \in X$, $s \in S$, $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = u_{k_1} \bmod p,\ \phi_2(k_2) = u_{k_2} \bmod p, \qquad (21)$$

$$\psi_1\left(x, \phi_1(k_1), k_2\right) = x \cdot u_{k_1+k_2} \bmod p = s,$$

$$\psi_2\left(s, \phi_2(k_2), k_1\right) = s \cdot u^{-1}_{k_2+k_1} \bmod p = x. \qquad (22)$$

Багатоосновну алгебру $\Omega_U \overset{def}{=} (X, S, K_1, K_2, D_1, D_2, \phi_1, \phi_2, \psi_1, \psi_2)$ назвемо криптосистемою асиметричного шифрування на основі U_k –послідовностей. Рівняння (17) буде виконуватись для U_k –послідовностей, оскільки з аналітичної залежності (7) видно, що $u_{n+m,k} = u_{m+n,k}$ для будь-яких цілих додатних n, m та k, і ці значення елементів можуть бути обчислені згідно залежності (7).

Стійкість криптосистеми Ω_U визначається складністю обчислення k_1 з $u_{k_1} \bmod p$ (або k_2 з $u_{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу

U_k –послідовності, обчисленого за модулем для великого значення індексу. В [12] показано, що ця задача є не менш складною, ніж задача обчислення дискретного логарифму в полі $GF(p)$.

Приклад 6. (система асиметричного шифрування на основі рекурентних V_k –послідовностей)

Якщо p – просте число, то покладемо $K_1 = K_2 = D_1 = D_2 = X = S = GF(p)$.

На основі математичного апарату рекурентних V_k –послідовностей визначимо сюр'єктивні відображення $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\psi_1 : X \times D_1 \times K_2 \to S$ та $\psi_2 : S \times D_2 \times K_1 \to X$ для усіх $x \in X$, $s \in S$, $k_1 \in K_1$, $k_2 \in K_2$ таким чином

$$\phi_1(k_1) = v_{k_1} \bmod p,\ \phi_2(k_2) = v_{k_2} \bmod p, \quad (23)$$

$$\psi_1\left(x, \phi_1(k_1), k_2\right) = x \cdot v_{k_1 \cdot k_2} \bmod p = s,$$

$$\psi_2\left(s, \phi_2(k_2), k_1\right) = s \cdot v^{-1}_{k_2 \cdot k_1} \bmod p = x. \quad (24)$$

Назвемо алгебру $\Omega_V \overset{def}{=} (X, S, K_1, K_2, D_1, D_2, \phi_1, \phi_2, \psi_1, \psi_2)$ криптосистемою асиметричного шифрування на основі V_k –послідовностей. Справедливість рівняння (17) буде виконуватись для V_k –послідовностей, оскільки $v_{n \cdot m,k} = v_{m \cdot n,k}$ і ці значення елементів можуть бути обчислені за модулем p за алгоритмом прискореного обчислення елементу V_k –послідовності з мультиплікативною зміною індексу [11] на основі аналітичної залежності (3) обчислення елементів $v_{n+m,k}$ для будь-яких цілих додатних n, m та k.

Стійкість криптосистеми Ω_V визначається складністю обчислення k_1 з $v_{k_1} \bmod p$ (або k_2 з $v_{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу V_k –послідовності, обчисленого за модулем для великого значення індексу. В [12] показано, що ця задача є не менш складною, ніж задача обчислення дискретного логарифму в полі $GF(p)$.

Алгебраїчні моделі автентифікації сторін взаємодії. Використовуючи багатоосновну універсальну алгебру, пропонується модель автентифікації сторін взаємодії представити у вигляді алгебраїчної конструкції з 7-ми скінчених непустих множин та 5-ти відображень, пов'язаних однією тотожністю: K_1 – множина секретних ключів претендента; D_1 – множина відкритих ключів претендента; K_2 – множина сеансових секретних ключів претендента; D_2 – множина відкритої сеансової ключової інформації претендента; K_3 – множина сеансових ключів перевіряльника; D_3 – множина відкритої сеансової ключової інформації перевіряльника; S – множина кодів автентичності претендента; $\phi_1 : K_1 \to D_1$, $\phi_2 : K_2 \to D_2$, $\phi_3 : K_3 \to D_3$ – сюр'єктивні відображення; $\psi_1 : K_1 \times K_2 \times D_3 \to S$, $\psi_2 : D_1 \times K_3 \times S \to D_2$ – сюр'єктивні відображення; причому для усіх $k_1 \in K_1$, $k_2 \in K_2$, $k_3 \in K_3$ виконується рівняння

$$\phi_2(k_2) = \psi_2\left(\phi_1(k_1), k_3, \psi_1\left(k_1, k_2, \phi_3(k_3)\right)\right). \quad (25)$$

Запропонована алгебраїчна конструкція автентифікації сторін взаємодії являє собою багатоосновну універсальну алгебру

$$\Lambda = \left(K_1, K_2, K_3, D_1, D_2, D_3, S, \phi_1, \phi_2, \phi_3, \psi_1, \psi_2\right). \quad (26)$$

Алгебра Λ вважається загальнодоступною. Автентифікація сторін взаємодії відбувається таким чином. Претендент, або центр довіри, вибирає секретний ключ $k_1 \in K_1$ та обчислює на його основі відкритий ключ $d_1 = \phi_1(k_1) \in D_1$, який шляхом відкритого публікування передається перевіряльнику. Коли претендент хоче довести свою автентичність перевіряльнику, він, повідомивши про це перевіряльника, обирає сеансовий секретний ключ $k_2 \in K_2$ та обчислює, використовуючи його, відкрите сеансове ключове значення $d_2 = \phi_2(k_2) \in D_2$. В цей час перевіряльник обирає свій сеансовий ключ $k_3 \in K_3$ та обчислює, використовуючи його, своє відкрите сеансове ключове значення $d_3 = \phi_3(k_3) \in D_3$, яке передає претенденту. Отримавши $d_3 \in D_3$ від перевіряльника, претендент обчислює код своєї автентичності як $s = \psi_1\left(k_1, k_2, d_3\right) \in S$ та передає його перевіряльнику разом з $d_2 \in D_2$. На завершення, перевіряльник, отримавши значення $s \in S$ та $d_2 \in D_2$, звіряє останнє значення шляхом обчислення $\psi_2\left(d_1, k_3, s\right) \in D_2$ та перевірки $d_2 = \psi_2\left(d_1, k_3, s\right)$. Виходячи з тотожності (25), перевіряльник таким чином має переконатись в справжності коду автентичності претендента.

Безпека представленої системи автентифікації сторін взаємодії на основі алгебри Λ базується на тому, що зловмисник має усю інформацію, яку надсилають претендент та перевіряльник один одному, має певні (обмежені) обчислювальні ресурси, але не може знайти секретний ключ претендента $k_1 \in K_1$ з тим, щоб видавати себе за претендента. Таким чином, безпека системи автентифікації визначається складністю вирішення

математичної задачі: за відомими значеннями $d_1 \in \phi_1(K_1) = D_1$, $d_2 \in \phi_2(K_2) = D_2$, $d_3 \in \phi_3(K_3) = D_3$, $s \in \psi_1(K_1, K_2, D_3) = S$, не знаючи $k_1 \in K_1$, $k_2 \in K_2$ і, можливо $k_3 \in K_3$, знайти невідомий елемент $k_1 \in K_1$. Таким чином, вимоги безпеки системи автентифікації сторін взаємодії означають, що складність вирішення цієї математичної задачі в даній алгебрі Λ є достатньо високою.

Слід також відзначити, що знаходження явного вигляду відображень ψ_1, ψ_2 та ϕ_1, ϕ_2, ϕ_3 є ще більш нетривіальною математичною задачею, ніж у моделях асиметричного криптографічного захисту, що розглядались вище, оскільки вже для п'яти функцій маємо всього одне функціональне співвідношення (25). Тому знаходження конкретних прикладів цих функцій є доволі складною задачею.

Прикладом запропонованої моделі автентифікації сторін взаємодії на основі алгебри Λ є криптографічна система Шнорра [15].

Приклад 7. (система автентифікації сторін взаємодії Шнорра)

Нехай p і q – прості числа, $q: q \mid p-1$; $GF(p) = \{0,1,..., p-1\}$ та $GF(q) = \{0,1,..., q-1\}$ – прості поля Галуа, $GF(q) \subset GF(p)$; $g \in Z_p^*$, $g \neq 1$: $g^q \equiv 1 (\mathrm{mod}\, p)$. Покладемо $K_1 = K_2 = K_3 = S = GF(q)$, $D_1 = D_2 = D_3 = GF(p)^*$.

Визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, ϕ_3: $K_3 \to D_3$, ψ_1: $K_1 \times K_2 \times D_3 \to S$ та ψ_2: $D_1 \times K_3 \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$, $k_3 \in K_3$ та $s \in S$ таким чином

$$\phi_1(k_1) = g^{-k_1} \bmod p,\ \phi_2(k_2) = g^{k_2} \bmod p,\ \phi_3(k_3) = k_3, \quad (27)$$

$$\psi_1(k_1, k_2, \phi_3(k_3)) = (k_2 + k_1 \cdot k_3) \bmod q = s,$$

$$\psi_2(\phi_1(k_1), k_3, s) = \left(g^{-k_1}\right)^{k_3} \cdot g^s \bmod p. \quad (28)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\Lambda_{SHN} \overset{def}{=} (K_1, K_2, K_3, D_1, D_2, D_3, S, \phi_1, \phi_2, \phi_3, \psi_1, \psi_2)$, яку назвемо криптосистемою автентифікації сторін взаємодії Шнорра, виконується рівняння (31).

Стійкість криптосистеми Λ_{SHN} визначається складністю обчислення k_1 з $g^{-k_1} \bmod p$ (або k_2 з $g^{k_2} \bmod p$). Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Щодо стійкості цієї криптосистеми слід також відзначити, що в криптосистемі Шнорра сеансовий ключ перевіряльника k_3 передається претенденту в явному вигляді, тобто $\phi_3(k_3) = k_3$. Це говорить про те, що криптосистема Шнорра хоч і має достатній рівень стійкості, але потенційно може існувати більш стійка криптосистема, в якій функція $\phi_3(k_3)$ буде обчислюватись за більш складним законом.

Запропонуємо модель автентифікації сторін взаємодії на основі алгебри Λ з використанням математичного апарату рекурентних V_k –послідовностей.

Приклад 8. (система автентифікації сторін взаємодії на основі рекурентних V_k –послідовностей)

Якщо p – просте число, то покладемо $K_1 = K_2 = K_3 = D_1 = D_2 = D_3 = S = GF(p)$, де $GF(p) = \{0,1,..., p-1\}$ – просте поле Галуа.

На основі математичного апарату рекурентних V_k –послідовностей визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, ϕ_3: $K_3 \to D_3$, ψ_1: $K_1 \times K_2 \times D_3 \to S$ та ψ_2: $D_1 \times K_3 \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$, $k_3 \in K_3$ та $s \in S$ таким чином

$$\phi_1(k_1) = v_{-k_1} \bmod p,\ \phi_2(k_2) = v_{k_2} \bmod p,$$

$$\phi_3(k_3) = v_{k_3} \bmod p, \quad (29)$$

$$\psi_1(k_1, k_2, \phi_3(k_3)) = v_{k_2 + k_3 \cdot k_1} \bmod p = s,$$

$$\psi_2(\phi_1(k_1), k_3, s) = v_{-k_1 \cdot k_3 + (k_2 + k_3 \cdot k_1)} \bmod p. \quad (30)$$

Назвемо алгебру $\Lambda_V \overset{def}{=} (K_1, K_2, K_3, D_1, D_2, D_3, S, \phi_1, \phi_2, \phi_3, \psi_1, \psi_2)$ криптосистемою автентифікації сторін взаємодії на основі V_k –послідовностей. Не важко пересвідчитись, що справедливість рівняння (25) для цієї криптосистеми буде виконуватись. При цьому існують усі необхідні для роботи криптосистеми Λ_V аналітичні залежності та процедури обчислення елементів V_k –послідовностей. Зокрема, існує можливість для великих значень індексів обчислювати для будь-яких цілих додатних n, m та k елементи $v_{n,k}$ та $v_{-n,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [10], елементи $v_{n+m,k}$ та $v_{-n+m,k}$ відповідно за аналітичними залежностями (3) та (5), елементи $v_{n \cdot m,k}$ та $v_{-n \cdot m,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [11].

Стійкість криптосистеми Λ_V визначається складністю обчислення k_1 з $v_{k_1} \bmod p$. Складність цієї задачі визначається обсягом трудовитрат знахо-

дження індексу елементу V_k –послідовності, обчисленого за модулем для великого значення індексу.

Щодо стійкості цієї криптосистеми також слід зазначити, що, на відміну від криптосистеми Λ_{SHN} Шнорра, де $\phi_3(k_3)=k_3$, тобто сеансовий ключ перевіряльника k_3 передається претенденту в явному вигляді, в криптосистемі Λ_V на основі V_k –послідовностей функція $\phi_3(k_3)$ є значно більш складнішою, оскільки являє собою не індекс k_3, а елемент V_k –послідовності з цим індексом, який обчислений за модулем p.

Слід також відзначити, що в разі необхідності зменшення обчислювальної складності процедури перевірки автентичності та некритичності вимог щодо високого рівня криптографічної стійкості, в криптосистемі Λ_V на основі V_k –послідовностей функція $\phi_3(k_3)$, як і у криптосистемі Шнорра, також може в явному вигляді приймати значення сеансового ключа k_3 перевіряльника, тобто $\phi_3(k_3)=k_3$.

Так само, якщо існує необхідність зменшення претендентом обчислювальної складності процедури формування коду автентичності і вимоги до високого рівня криптостійкості не є критичними, то обчислюватись і передаватись перевіряльнику може не елемент $v_{k_2+k_3\cdot k_1} \bmod p$, що визначає s, а лише індекс $k_2+k_3\cdot k_1$ цього елементу, при цьому сам елемент буде обчислюватись на стороні перевіряльника і, в такому випадку, буде $\psi_1\left(k_1,k_2,\phi_3(k_3)\right)=k_2+k_3\cdot k_1=s$.

Алгебраїчні моделі цифрового підписування. Розглянемо тепер можливість побудови моделі цифрового підписування на основі універсальної алгебри. Використовуючи ідею перетворення криптосистеми автентифікації сторін взаємодії у криптосистему цифрового підписування [16], модель цифрового підписування може бути побудована як модель автентифікації сторін взаємодії, в якій замість сеансового ключа k_3 перевіряльника використовується претендентом значення певного відображення множини X повідомлень, що підписуються. При цьому можливі варіанти, коли це відображення визначається або на основі множин D_2 та X, тобто множиною відкритої сеансової ключової інформації претендента та множиною повідомлень, або на основі лише самої множини X повідомлень, що підписуються.

Виходячи з цього, спочатку побудуємо модель цифрового підписування на основі багатоосновної універсальної алгебри для першого варіанту.

Пропонуємо модель цифрового підписування представити у вигляді алгебраїчної конструкції з 7-ми скінчених непустих множин та 5-ти відображень, пов'язаних однією тотожністю: K_1 – множина секретних ключів відправника-підписанта повідомлень; D_1 – множина відкритих ключів підписанта; K_2 – множина сеансових секретних ключів підписанта; D_2 – множина відкритої сеансової ключової інформації підписанта; X – множина повідомлень, що підписуються; Y – множина хешованої інформації; S – множина підписів; $\phi_1\colon K_1\to D_1$, $\phi_2\colon K_2\to D_2$ – сюр'єктивні відображення; $\varphi\colon D_2\times X\to Y$, $\psi_1\colon K_1\times K_2\times Y\to S$, $\psi_2\colon D_1\times Y\times S\to D_2$ – сюр'єктивні відображення; причому для усіх $k_1\in K_1$, $k_2\in K_2$ та $x\in X$ виконується рівняння

$$\phi_2(k_2)=\psi_2\left(\phi_1(k_1),\varphi\left(\phi_2(k_2),x\right),\psi_1\left(k_1,k_2,\varphi\left(\phi_2(k_2),x\right)\right)\right). \quad (31)$$

Запропонована алгебраїчна конструкція цифрового підписування являє собою багатоосновну універсальну алгебру

$$\Im=\left(K_1,K_2,D_1,D_2,X,Y,S,\phi_1,\phi_2,\varphi,\psi_1,\psi_2\right). \quad (32)$$

Алгебра $\Im$ вважається загальнодоступною. Цифрове підписування відбувається таким чином. Відправник-підписант повідомлень, або центр довіри, вибирає секретний ключ $k_1\in K_1$ та обчислює на його основі відкритий ключ $d_1=\phi_1(k_1)\in D_1$, який шляхом відкритого публікування передається одержувачу-перевіряльнику. Коли відправник хоче підписати своє повідомлення $x\in X$ та передати його разом з підписом перевіряльнику, він обирає сеансовий секретний ключ $k_2\in K_2$ та обчислює, використовуючи його, відкрите сеансове ключове значення $d_2=\phi_2(k_2)\in D_2$. Далі відправник спочатку хешує повідомлення $x\in X$ та щойно отримане ним значення $d_2\in D_2$, обчислюючи $y=\varphi\left(d_2,x\right)\in Y$, а потім обчислює підпис $s=\psi_1\left(k_1,k_2,y\right)\in S$ і передає обчислені значення $y\in Y$ та $s\in S$ разом з повідомленням $x\in X$ одержувачу-перевіряльнику. Після цього одержувач спочатку обчислює $d_2=\psi_2\left(d_1,y,s\right)\in D_2$, потім хешує це значення разом з повідомленням $x\in X$ за допомогою $\varphi\left(d_2,x\right)\in Y$ і звіряє обчислене значення з отриманим від відправника значенням $y\in Y$. Виходячи з тотожності (31), перевіряльник таким чином має переконатись у справжності підпису відправника.

Безпека представленої системи цифрового підписування на основі алгебри $\Im$ базується на тому, що зловмисник має усю інформацію, яку надсилає відправник-підписант одержувачу-перевіряльнику, має певні (обмежені) обчислювальні ресурси, але не може знайти секретний ключ підписанта $k_1 \in K_1$ з тим, щоб підписувати свої повідомлення і видавати їх за повідомлення відправника. Таким чином, безпека системи цифрового підписування визначається складністю вирішення математичної задачі: за відомими значеннями $d_1 \in \phi_1(K_1) = D_1$, $d_2 \in \phi_2(K_2) = D_2$, $y \in \varphi(D_2, X) = Y$, $s \in \psi_1(K_1, K_2, Y) = S$, не знаючи $k_1 \in K_1$ та $k_2 \in K_2$, знайти невідомий елемент $k_1 \in K_1$. Таким чином, вимоги безпеки системи автентифікації сторін взаємодії означають, що складність вирішення цієї математичної задачі в даній алгебрі $\Im$ є достатньо високою.

Знаходження явного вигляду відображень ψ_1, ψ_2, φ та ϕ_1, ϕ_2 алгебри $\Im$, які б задовольняли функціональному співвідношенню (31) є настільки ж складною і нетривіальною задачею, що і знаходження явного вигляду відображень ψ_1, ψ_2 та ϕ_1, ϕ_2, ϕ_3 для моделі автентифікації сторін взаємодії на основі алгебри Λ, які задовольняли б функціональному співвідношенню (25).

Прикладом запропонованої моделі цифрового підписування на основі алгебри $\Im$ є криптографічна система Шнорра [15].

Приклад 9. (система цифрового підписування Шнорра)

Нехай p і q – прості числа, $q: q \mid p-1$; $GF(p) = \{0,1,..., p-1\}$ та $GF(q) = \{0,1,..., q-1\}$ – прості поля Галуа, $GF(q) \subset GF(p)$; $g \in Z_p^*$, $g \neq 1$: $g^q \equiv 1 (\mathrm{mod}\, p)$. Покладемо $K_1 = K_2 = Y = S = GF(q)$, $D_1 = D_2 = GF(p)^*$, $X = GF(p)$.

Визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, φ: $D_2 \times X \to Y$, ψ_1: $K_1 \times K_2 \times Y \to S$ та ψ_2: $D_1 \times Y \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ та $x \in X$ таким чином

$$\phi_1(k_1) = g^{-k_1} \bmod p,\ \phi_2(k_2) = g^{k_2} \bmod p,$$
$$\varphi(\phi_2(k_2), x) = h\left(\left(g^{k_2} \bmod p\right) \| x\right) = y, \qquad (33)$$

де $h: \{0,1\}^* \to Z_q$ – функція хешування,

$$\psi_1(k_1, k_2, y) = (k_2 + k_1 \cdot y) \bmod q = s,$$
$$\psi_2(\phi_1(k_1), y, s) = \left(g^{-k_1}\right)^y \cdot g^s \bmod p. \qquad (34)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\Im_{SHN} \overset{def}{=} (K_1, K_2, D_1, D_2, X, Y, S, \phi_1, \phi_2, \varphi, \psi_1, \psi_2)$, яку назвемо криптосистемою цифрового підписування Шнорра, виконується рівняння (31).

Стійкість криптосистеми $\Im_{SHN}$ визначається складністю обчислення k_1 з $g^{-k_1} \bmod p$ або k_2 з $g^{k_2} \bmod p$. Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Запропонуємо модель цифрового підписування на основі алгебри $\Im$ з використанням математичного апарату рекурентних V_k–послідовностей.

Приклад 10. (система цифрового підписування на основі рекурентних V_k–послідовностей)

Якщо p – просте число, то покладемо $K_1 = K_2 = D_1 = D_2 = X = Y = S = GF(p)$, де $GF(p) = \{0,1,..., p-1\}$ – просте поле Галуа.

На основі математичного апарату рекурентних V_k–послідовностей визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, φ: $D_2 \times X \to Y$, ψ_1: $K_1 \times K_2 \times Y \to S$ та ψ_2: $D_1 \times Y \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ та $x \in X$ таким чином

$$\phi_1(k_1) = v_{-k_1} \bmod p,\ \phi_2(k_2) = v_{k_2} \bmod p,$$
$$\varphi(\phi_2(k_2), x) = h\left(x \left\| \left(v_{k_2} \bmod p\right)\right.\right) = y, \qquad (35)$$

де $h: \{0,1\}^* \to Z_p$ – функція хешування,

$$\psi_1(k_1, k_2, y) = v_{k_2 + k_1 \cdot y} \bmod p = s,$$
$$\psi_2(\phi_1(k_1), y, s) = v_{-k_1 \cdot y + (k_2 + k_1 \cdot y)} \bmod p. \qquad (36)$$

Назвемо алгебру $\Im_V \overset{def}{=} (K_1, K_2, D_1, D_2, X, Y, S, \phi_1, \phi_2, \varphi, \psi_1, \psi_2)$ криптосистемою цифрового підписування на основі V_k–послідовностей. Не важко пересвідчитись, що справедливість рівняння (31) для цієї криптосистеми буде виконуватись. При цьому існують усі необхідні для роботи криптосистеми $\Im_V$ аналітичні залежності та процедури обчислення елементів V_k–послідовностей, а саме існує можливість для великих значень індексів обчислювати для будь-яких цілих додатних n, m та k елементи $v_{n,k}$ та $v_{-n,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [10], елементи $v_{n+m,k}$ та $v_{-n+m,k}$ відповідно за аналітичними залежностями (3) та (5), елементи $v_{n \cdot m,k}$ та $v_{-n \cdot m,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [11].

Стійкість криптосистеми $\Im_V$ визначається складністю обчислення k_1 з $v_{-k_1} \bmod p$. Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу V_k –послідовності, обчисленого за модулем для великого значення індексу.

Тут слід відзначити, що в разі необхідності зменшення обчислювальної складності процедури формування підпису відправником і некритичності вимог щодо високого рівня криптографічної стійкості, обчислюватись і передаватись одержувачу може не елемент $v_{k_2+k_1\cdot y} \bmod p$, що визначає s, а лише індекс $k_2 + k_1 \cdot y$ цього елементу, при цьому сам елемент буде обчислюватись на стороні одержувача і, в такому випадку, буде $\psi_1(k_1, k_2, y) = k_2 + k_1 \cdot y = s$.

Також слід зазначити, що відображення $\varphi(\phi_2(k_2), x) \in Y$, яке визначає y згідно (35) як $h\left(x \| \left(v_{k_2} \bmod p\right)\right)$, може мати й інші варіанти обчислення, наприклад як $h(x) \cdot v_{k_2} \pmod p$.

Як вже зазначалось вище, можливий ще один варіант алгебри $\Im$ цифрового підписування, коли хешована інформація Y буде визначатись відображенням φ не на основі множин повідомлень X та відкритої сеансової ключової інформації D_2 відправника, а лише на основі однієї множини повідомлень X. При цьому множина підписів S буде визначатись відображенням формування підписів ψ_1 на основі множин секретних ключів відправника K_1 та K_2, а також множиною хешованої інформації Y та окремо множиною відкритої сеансової ключової інформації D_2. Так само відображення перевірки підписів ψ_2 буде визначатись на основі множин відкритих ключів D_1, підписів S, хешованої інформації Y та множини відкритої сеансової ключової інформації відправника D_2.

В такому варіанті алгебри $\Im$ сюр'єктивні відображення φ, ψ_1 та ψ_2 будуть визначатись як φ: $X \to Y$, ψ_1: $K_1 \times K_2 \times D_2 \times Y \to S$, ψ_2: $D_1 \times D_2 \times Y \times S \to D_2$ і для усіх $k_1 \in K_1$, $k_2 \in K_2$ та $x \in X$ повинно виконуватись таке рівняння

$$\phi_2(k_2) = \psi_2\left(\phi_1(k_1), \phi_2(k_2), \varphi(x), \psi_1\left(k_1, k_2, \phi_2(k_2), \varphi(x)\right)\right). \quad (37)$$

Прикладом запропонованої моделі цифрового підписування на основі такого варіанту алгебри $\Im$ є криптографічна система Ель-Гамаля [14].

Приклад 11. (система цифрового підписування Ель-Гамаля)

Нехай p – просте число; $GF(p) = \{0,1,..., p-1\}$ – просте поле Галуа; $g \in Z_p^*$. Покладемо $K_1 = K_2 = D_1 = D_2 = GF(p)^*$, $X = Y = S = GF(p)$.

Визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, φ: $X \to Y$, ψ_1: $K_1 \times K_2 \times D_2 \times Y \to S$ та ψ_2: $D_1 \times D_2 \times Y \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$: $НСД(k_2, p-1) = 1$ та $x \in X$ таким чином

$$\phi_1(k_1) = g^{k_1} \bmod p = d_1,\ \phi_2(k_2) = g^{k_2} \bmod p = d_2,$$
$$\varphi(x) = h(x) = y, \quad (38)$$

де h: $\{0,1\}^* \to Z_p$ – функція хешування,

$$\psi_1(k_1, k_2, d_2, y) = k_2^{-1} \cdot (y - k_1 \cdot d_2) \bmod (p-1) = s,$$
$$\psi_2(d_1, d_2, y, s) = d_1^{d_2} \cdot d_2^{s+1} \cdot g^{-y} \bmod p. \quad (39)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\Im_{EG} \overset{def}{=} (K_1, K_2, D_1, D_2, X, Y, S, \phi_1, \phi_2, \varphi, \psi_1, \psi_2)$, яку назвемо криптосистемою цифрового підписування Ель-Гамаля, виконується рівняння (37).

Стійкість криптосистеми $\Im_{EG}$ визначається складністю обчислення k_1 з $g^{k_1} \bmod p$ або k_2 з $g^{k_2} \bmod p$. Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Ще одним прикладом запропонованої моделі цифрового підписування на основі другого варіанту алгебри $\Im$ є криптографічна система DSA [17].

Приклад 12. (система цифрового підписування DSA)

Нехай p і q – прості числа, q: $q | p-1$; $GF(p) = \{0,1,..., p-1\}$ та $GF(q) = \{0,1,..., q-1\}$ – прості поля Галуа, $GF(q) \subset GF(p)$; $g \in Z_p^*$, $g \neq 1$: $g^q \equiv 1 (\bmod p)$. Покладемо $K_1 = K_2 = Y = S = GF(q)$, $D_1 = D_2 = GF(p)^*$, $X = GF(p)$.

Визначимо сюр'єктивні відображення ϕ_1: $K_1 \to D_1$, ϕ_2: $K_2 \to D_2$, φ: $X \to Y$, ψ_1: $K_1 \times K_2 \times D_2 \times Y \to S$ та ψ_2: $D_1 \times D_2 \times Y \times S \to D_2$ для усіх $k_1 \in K_1$, $k_2 \in K_2$ та $x \in X$ таким чином

$$\phi_1(k_1) = g^{k_1} \bmod p = d_1,$$
$$\phi_2(k_2) = \left(g^{k_2} \bmod p\right) \bmod q = d_2,$$
$$\varphi(x) = h(x) = y, \quad (40)$$

де h: $\{0,1\}^* \to Z_q$ – функція хешування,

$$\psi_1(k_1,k_2,d_2,y)=k_2^{-1}\cdot(y+k_1\cdot d_2)\bmod q=s,$$
$$\psi_2(d_1,d_2,y,s)=\left(d_1^{s^{-1}\cdot d_2}\cdot g^{s^{-1}\cdot y}\bmod p\right)\bmod q. \quad (41)$$

Не важко пересвідчитись, що в багатоосновній алгебрі $\Im_{DSA}\overset{def}{=}(K_1,K_2,D_1,D_2,X,Y,S,\phi_1,\phi_2,\varphi,\psi_1,\psi_2)$, яку назвемо криптосистемою цифрового підписування DSA, виконується рівняння (37).

Стійкість криптосистеми $\Im_{DSA}$ визначається складністю обчислення k_1 з $g^{k_1}\bmod p$ або k_2 з $\left(g^{k_2}\bmod p\right)\bmod q$. Складність цієї задачі визначається обсягом трудовитрат на вирішення задачі обчислення дискретного логарифму в полі $GF(p)$.

Запропонуємо тепер модель цифрового підписування на основі другого варіанту алгебри $\Im$ з використанням математичного апарату рекурентних V_k –послідовностей.

Приклад 13. (система цифрового підписування на основі рекурентних V_k –послідовностей (другий варіант)

Якщо p – просте число, то покладемо $K_1=K_2=D_1=D_2=X=Y=S=GF(p)$, де $GF(p)=\{0,1,...,p-1\}$ – просте поле Галуа.

На основі математичного апарату рекурентних V_k –послідовностей визначимо сюр'єктивні відображення $\phi_1\colon K_1\to D_1$, $\phi_2\colon K_2\to D_2$, $\varphi\colon X\to Y$, $\psi_1\colon K_1\times K_2\times D_2\times Y\to S$ та $\psi_2\colon D_1\times D_2\times Y\times S\to D_2$ для усіх $k_1\in K_1$, $k_2\in K_2$ та $x\in X$ таким чином

$$\phi_1(k_1)=v_{-k_1}\bmod p=d_1,$$
$$\phi_2(k_2)=v_{-k_2}\bmod p=d_2,$$
$$\varphi(x)=h(x)=y, \quad (42)$$

де $h\colon\{0,1\}^*\to Z_p$ – функція хешування,

$$\psi_1(k_1,k_2,d_2,y)=v_{k_2\cdot y+k_1\cdot d_2}\bmod p=s,$$
$$\psi_2(d_1,d_2,y,s)=v_{-k_1\cdot d_2+(k_2\cdot y+k_1\cdot d_2)-k_2\cdot(y+1)}\bmod p. \quad (43)$$

Назвемо алгебру $\Im_{V'}\overset{def}{=}(K_1,K_2,D_1,D_2,X,Y,S,\phi_1,\phi_2,\varphi,\psi_1,\psi_2)$ криптосистемою цифрового підписування на основі V_k –послідовностей (другий варіант). Не важко пересвідчитись, що справедливість рівняння (37) для цієї криптосистеми буде виконуватись. При цьому існують усі необхідні для роботи криптосистеми $\Im_{V'}$ аналітичні залежності та процедури обчислення елементів V_k - послідовностей, а саме існує можливість для великих значень індексів обчислювати для будь-яких цілих додатних n, m та k елементи $v_{n,k}$ та $v_{-n,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [10], елементи $v_{n+m,k}$, $v_{n-m,k}$ та $v_{-n+m,k}$ відповідно за аналітичними залежностями (3), (4) та (5), елементи $v_{n\cdot m,k}$ та $v_{-n\cdot m,k}$ за відповідними алгоритмами прискореного обчислення цих елементів [11].

Стійкість криптосистеми $\Im_{V'}$ визначається складністю обчислення k_1 з $v_{-k_1}\bmod p$. Складність цієї задачі визначається обсягом трудовитрат знаходження індексу елементу V_k –послідовності, обчисленого за модулем для великого значення індексу.

Слід зазначити, що, як і у криптосистемі $\Im_V$, в разі необхідності зменшення у криптосистемі $\Im_{V'}$ обчислювальної складності процедури формування підпису відправником і некритичності вимог щодо високого рівня криптографічної стійкості, обчислюватись і передаватись одержувачу може не елемент $v_{k_2\cdot y+k_1\cdot d_2}\bmod p$, що визначає s, а лише індекс $k_2\cdot y+k_1\cdot d_2$ цього елементу, при цьому сам елемент буде обчислюватись на стороні одержувача і, в такому випадку, буде $\psi_1(k_1,k_2,d_2,y)=k_2\cdot y+k_1\cdot d_2=s$.

Також слід відзначити, що окрім $k_2\cdot y+k_1\cdot d_2$ існують й інші варіанти конструкцій обчислень індексу елементу V_k –послідовності, що визначає s, наприклад $k_2\cdot y-k_1\cdot d_2$, $-k_2\cdot y+k_1\cdot d_2$, $k_1\cdot y+k_2\cdot d_2$, $k_1\cdot y-k_2\cdot d_2$, $-k_1\cdot y+k_2\cdot d_2$ та інші. Відповідним чином буде змінюватись і функція перевірки підпису $\psi_2(d_1,d_2,y,s)$.

Висновки. Розглянуто модель pk –алгебри, що узагальнює відомі системи відкритого розподілу секретних ключів. Запропоновано алгебраїчні моделі Ω, Λ та $\Im$ відповідно асиметричного шифрування, автентифікації сторін взаємодії та цифрового підписування як багатоосновні універсальні алгебри. Для цифрового підписування представлено два варіанта алгебри $\Im$, коли множина хешованої інформації визначається або множиною повідомлень, що підписуються, та відкритої сеансової ключової інформації відправника, або лише множиною повідомлень. Розглянуто моделі існуючих криптосистем на основі алгебри A розподілу секретних ключів та запропонованих алгебр Ω, Λ та $\Im$ відповідно шифрування, автентифікації та цифрового підписування. Запропоновано моделі розподілу секретних ключів та асиметричного шифрування відповідно на основі алгебр A та Ω з використан-

ням математичного апарату рекурентних U_k – та V_k –послідовностей. Запропоновано різні варіанти моделей автентифікації сторін взаємодії та цифрового підписування відповідно на основі алгебр Λ та $\Im$ з використанням математичного апарату рекурентних V_k –послідовностей. Запропоновані варіанти моделей автентифікації та цифрового підписування на основі V_k –послідовностей в різних випадках забезпечують спрощення обчислення та підвищення криптографічної стійкості у порівняні з відомими аналогами.

ЛІТЕРАТУРА

[1]. Shannon C.E. Communications theory of secrecy systems // Bell Systems Technical Journal. – №28, 1949. – P. 656–715.

[2]. Кон П. Универсальная алгебра. – М.: Мир, 1969. – 351 с.

[3]. Мальцев А.И. Алгебраические системы. – М.: Наука, 1970. – 392 с.

[4]. Артамонов В.А., Ященко В.В. Многоосновные алгебры в системах открытого шифрования // Успехи матем. наук. – Т. 49, 1994. – С. 149–150.

[5]. Сидельников В.М., Черепнев М.А., Ященко В.В. Системы открытого распределения ключей на основе некоммутативных полугрупп // Доклады РАН. – Т. 332, № 5, 1993. – С. 566–567.

[6]. Алексейчук А., Пришлин С., Романов А. Алгебраические модели криптографических систем с открытым ключом // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Випуск 3, 2001. – С. 140–144.

[7]. Алексейчук А.Н., Романов А.И. Регулярные конгруэнции и строение алгебраических моделей симметричных криптосистем // Радиотехника. – Вып. 126, 2002. – С. 42–58.

[8]. Яремчук Ю.Є. Криптографічні методи та засоби шифрування інформації на основі рекурентних послідовностей: Монографія. – Вінниця : Книга-Вега, 2002. – 136 с.

[9]. Яремчук Ю.Є. Аналітичні залежності прискореного обчислення елементів рекурентних послідовностей для можливості побудови методів автентифікації та цифрового підписування // Інформатика та математичні методи в моделюванні. – Том 3, №4, 2013. – С. 306–313.

[10]. Яремчук, Ю.Є. Розробка алгоритмів прискореного обчислення елементів рекурентних послідовностей для криптографічних застосувань // Реєстрація, зберігання і обробка даних. – Т. 15, №1, 2013. – С. 14–22.

[11]. Яремчук Ю.Є. Методи та алгоритми прискореного обчислення елементів рекурентних послідовностей з мультиплікативною зміною індексів // Вісник Східноукраїнського національного університету імені Володимира Даля. – №17 (206), Частина 2, 2013. – С. 12–16.

[12]. Яремчук Ю.Є. Оцінювання криптостійкості методів шифрування інформації на основі рекурентних послідовностей // Східно-Європейський журнал передових технологій. – №2/10(62), 2013. – С. 35–38.

[13]. W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.

[14]. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE Intern. Symp. Informat. Theory. – 1985. – V.IT–31. №4. – P. 469–472.

[15]. Schnorr C.P. Efficient Signature Generation for Smart Cards // Advances in Cryptology – CRYPTO'89 Proceedings, Springer-Verlag, Lecture Notes in Computer Science. – Nr 435, 1990. – Pp. 239-252.

[16]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

[17]. National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard", U.S. Department of Commerce, May 1994.

REFERENCES

[1]. Shannon, C.E. (1949). Communications theory of secrecy systems. *Bell Systems Technical Journal*, 28, p. 656-715.

[2]. Kon, P. (1969). Universal algebra. Moscow: Mir.

[3]. Malcev, A.I. (1970). Algebraic systems. Moscow: Nauka.

[4]. Artamonov, V.A., Yaschenko, V.V. (1994). Polybasic algebras in public key encryption systems. *Advances of Mathematical Sciences*, V.49, p. 149-150.

[5]. Sidelnikov, V.M., Cherepnev, M.A., Yaschenko, V.V. (1993). Public key distribution system based on noncommutative semigroups. *RAS reports*, V.332, №5, p. 566-567.

[6]. Alexeychuk, A.N., Prishlin, S., Romanov, A.I. (2001). Algebraic models of public key cryptographic systems. *Legal, regulatory and metrological support for the system for information security in Ukraine*, 3, p. 140-144.

[7]. Alexeychuk, A.N., Romanov, A.I. (2002). Regular congruences and configuration of algebraic models of symmetric cryptographic systems. *Radiotekhnika*, 126, p. 42-58.

[8]. Iaremchuk, I.E. (2002). Cryptographic methods and ways of information encryption, based on recurrent sequences: a monograph. Vinnytsia: Knyga-Vega.

[9]. Iaremchuk, I.E. (2013). Analytical dependences of the accelerated elements computing of recurrent sequences to enable building methods of authentication and digital signature. *Informatics and mathematical methods in modeling*, V.3, №4, p. 306-313.

[10]. Iaremchuk, I.E. (2013). Development of algorithms for accelerated computation of elements of recurrent

sequences for cryptographic purposes. *Data registration, saving and processing,* V.15, №1, p. 14-22.
[11]. Iaremchuk, I.E. (2013). Methods and algorithms of accelerated computing of the recurrent sequences elements with multiplicated index change. *Bulletin of the East Ukrainian National University*, №17(206), Part 2, p. 12-16.
[12]. Iaremchuk, I.E. (2013). Evaluation of cryptographic reliability of information encryption methods based on recurrent sequences. *Eastern-European Journal of Enterprise Technologies*, №2/10(62), p. 35-38.
[13]. Diffie, W., Hellman, M.E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, №22, p. 644-654.
[14]. El Gamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Intern. Symp. Informat. Theory*, V.IT–31, №4, p. 469-472.
[15]. Schnorr, C.P. (1990). Efficient Signature Generation for Smart Cards. *Advances in Cryptology – CRYPTO'89 Proceedings, Springer-Verlag, Lecture Notes in Computer Science*, Nr 435, p. 239-252.
[16]. Schneier, B. (2002). Applied Cryptography. Protocols, Algorithms and Source Code in C. Moscow: Triumf.
[17]. National Institute of Standards and Technology. (1994). Digital Signature Standard, *NIST FIPS PUB 186, U.S. Department of Commerce*.

АЛГЕБРАИЧЕСКИЕ МОДЕЛИ АССИМЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

Моделирование криптографических методов на уровне алгебраических структур дает возможность более глубоко понять принципы их построения, особенности функционирования, исследовать их свойства. Существующие на сегодня алгебраические модели ассиметричных криптографических систем не обеспечивают в полной мере возможности их использования. В работе рассмотрено алгебраическую модель открытого распределения секретных ключей, а также предложены алгебраические модели ассиметричного шифрования, аутентификации сторон взаимодействия и цифрового подписания как многоосновные универсальные алгебры. На основе представленных алгебр рассмотрены модели существующих криптосистем, а также предложены модели распределения секретных ключей и ассиметричного шифрования с использованием математического аппарата рекуррентных U_k– и V_k–последовательностей. Предложены различные варианты моделей аутентификации сторон взаимодействия и цифрового подписания с использованием математического аппарата рекуррентных V_k–последовательностей, которые в разных случаях обеспечивают упрощение вычислений и повышение криптографической стойкости по сравнению с известными аналогами.

Ключевые слова: криптография, алгебраические модели, распределение ключей, ассиметричное шифрование, аутентификация сторон взаимодействия, цифровое подписание.

ALGEBRAIC MODELS OF ASYMMETRIC CRYPTOGRAPHIC SYSTEMS

Modeling cryptographic methods on the level of algebraic structures enables a deeper understanding of the principles of their construction, operation features, and exploring their properties. The existing algebraic models of asymmetric cryptographic systems do not provide the full possibilities of their use. We consider an algebraic model of public distribution of secret keys, as well as an algebraic model of asymmetric encryption, authentication of interaction parties and digital signing as polybasic universal algebras. Based on the presented algebras, we considered existing cryptosystem models, as well as proposed models of distribution of secret keys and asymmetric encryption, using mathematical tools of recurrent U_k–and V_k sequences. We proposed a different version of the authentication model of interaction parties and of digital signing, using mathematical tools of recurrent V_k sequences, which in different occasions provide a simplification of computation, and enhance cryptographic reliability compared with the known analogs.

Keywords: cryptography, algebraic models, distribution of keys, asymmetric encryption, authentication of interaction parties, digital signing.

Яремчук Юрій Євгенович, кандидат технічних наук, доцент, директор Центру інформаційних технологій і захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
E-mail: yurevyar@vntu.net.
Яремчук Юрий Евгеньевич, кандидат технических наук, доцент, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Iurii Iaremchuk, Ph.D., associate professor, Director of IT and Information Security Center, Professor Department of Management and Security of Information Systems of Vinnytsia National Technical University.