УДК 004.056.5 DOI: 10.26565/2519-2310-2020-2-04

СПОСІБ КРИПТОЛОГІЧНИХ ПЕРЕТВОРЕНЬ ДАНИХ

Михайло Сукнов[1], Ігор Громико[2], Євгеній Перчик

[1] Харківський національний університет радіоелектроніки. пр. Науки, 14, Харків, 61166, Україна
[2] Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
mykhailo.suknov@nure.ua, i.gromyko@karazin.ua

Рецензент: Володимир Максимович, д.т.н., проф., Національний університет «Львівська політехніка», м. Львів, 79013, Україна.
vmax@polynet.lviv.ua

Поступила: Липень 2020.

Анотація: *Протидія квантовому комп'ютеру в процесі неповноважного надшвидкісного розшифрування повідомлень - технічно здійсненна. Власник інформації повинен протиставити комп'ютеру конкурента завдання, вирішення яких потребує нескінченне число операцій при її дешифруванні. Наприклад, - залежність функцій від нескінченного числа інформативних ознак. Власник шифрує шляхом інтегрування функцій, одержувач дешифрує рішенням інтегральних рівнянь. В цьому разі превалює не дискретний, а аналоговий підхід. Базис для реалізації такого підходу створили польські вчені. Математик Стефан Банах (Stefan Banach, 1892-1945), який створив сучасний функціональний аналіз і Маріан Мазур (Marian Mazur, 1909-1983) автор «Якісної теорії інформації». Їх теорія була створена на противагу «Кількісної теорії інформації». Фахівці з криптології, які все життя присвятили вдосконаленню «дискретної» теорії і виявилися наближеними до влади (і фінансів), намагаються не згадувати, що Клод Шеннон у своїй фундаментальній роботі «Теорія зв'язку в секретних системах» неодноразово підкреслив дискретну спрямованість своїх розробок, попередивши майбутніх дослідників про специфічну обмеженість своєї роботи, яка адаптована до теорії зв'язку. Забуваючи про необмежені швидкості і обсяги пам'яті квантових комп'ютерів, ортодокси говорять про надмірність, та інші суто технічні моменти,застосовуючи проти своїх опонентів всі можливі важелі протидії. Прогрес науки зупинити неможливо. Дослідження показали реальність створення подібних криптографічних систем постквантового рівня.*

Ключові слова*: криптологія; квантовий комп'ютер; технології автоматизованого шифрування - дешифрування.*

1 Вступ

Спосіб, що розглядається в межах даної роботи, відноситься до області криптологічних способів та пристроїв для шифрування, та дешифрування повідомлень (*інформації*).

Відомо, що існує спосіб аналітичних криптологічних перетворень за допомогою матриць [1]. У цьому способі для реалізації шифрування даних цілочислова квадратна матриця множиться на вектор, елементи якого є номерами букв алфавіту. Відповідно при дешифруванні проводиться аналогічна процедура з використанням зворотної матриці, отриманої відомим способом. Недоліком даного способу є низький порядок матриць, що обумовлений обмеженістю обчислювальної потужності використовуваних технічних засобів [2], а також – неможливість шифрування неперервних функціональних залежностей.

У вищезазначеному способі криптологічні перетворення даних здійснюються шляхом дії оператора (у формі цілочисельної квадратної матриці) на вектор-строчку частини повідомлення з можливістю наступного дешифрування, шляхом реалізації аналогічної процедури з використанням зворотної матриці.

З огляду на все вищесказане, автори даної роботи пропонують розглянути новий спосіб криптологічних перетворень даних, які мають форму неперервних однозначних функціональних залежностей. Згідно попередньому задуму, шифрування повинно здійснюватися шляхом впливу на безперервну функцію повідомлення відповідним оператором, що представляє собою інтеграл з замкненим ядром, в який перетворюється матриця, коли її порядок спрямовується до нескінченності. Це призводить до інтегрального рівняння Фредгольма першого роду, для якого існує ефективний алгоритм чисельної реалізації. При цьому повідомлення являє собою і/або – аналітичну функціональну залежність, та/або – запис мовного сигналу як безперервного графіка, та/або – повідомлення, що являє собою фрагмент відео-зображення,

та/або – повідомлення, що являє собою букви алфавіту і інші символи, яким поставлені у відповідність неперервні однозначні функції, та/або – повідомлення, що являє собою таблицю, дискретні значення якої попередньо підлягають апроксимації, перетворюючись у неперервну однозначну аналітичну залежність.

Крім того, додатково, можна підбирати інтегральний оператор таким чином, щоб зворотний йому оператор, був раціональний в сенсі ефективності процедури дешифрування, а саме – вирішення відповідного інтегрального рівняння у аналітичному вигляді, прийнятному для процедури обчислювання.

2. Основна частина

Сутність вирішуваного завдання полягає в тому, що при представленні даних у формі алфавіту відсутня можливість передачі даних у інших неперервних формах представлення, наприклад, графіків функцій, відео зображення, таблиць, запису мовного сигналу.

В даному випадку під даними розуміються:

- відео-зображення по типу кардіограм, гістограм і т.п., а також елементи, які в комплексі складають графіки більш складного виду (*неоднозначно залежать від змінної*);
- таблиця чисел, яка за допомогою апроксимації (інтерполяції) може бути представлена у вигляді аналітичного виразу або графіка;
- текст, що містить букви, слова, числа, формули та інші позначення, які можуть бути представлені у вигляді графіка, наприклад, амплітуди акустичного тиску запису мовного сигналу;
- аналогічний попередньому текст, в якому кожному елементарному позначенню (*букви, числа, пробілу і т.і.*), ставиться у відповідність безперервна функція змінної, наприклад,

$$\psi_s(x) = c_s \sin \omega x, \tag{1}$$

де c_s – амплітуда, довільно встановлена різною для кожного $s = 1,2\ldots$.

Представлення даних у визначених формах забезпечує подальше їх аналітичне перетворення за допомогою математичного апарату безперервного аналізу, а саме, диференційного та інтегрального числення.

Згідно з пропозицією, шифрування здійснюється шляхом впливу на безперервну функцію повідомлення оператором, що представляє собою інтеграл з замкненим ядром, в який перетворюється матриця, коли її порядок спрямовується до нескінченності, що призводить до інтегрального рівняння Фредгольма 1-го роду, для якого існує ефективний алгоритм чисельної реалізації.

В якості прототипу автори пропонують використовувати відомий метод (спосіб) аналітичного шифрування на основі матричного аналізу [1, с. 20-22]. В такому випадку слова розбиваються на блоки з *n* букв (*у наведеному прикладі* $n = 3$). Кожній букві ставиться у відповідність її номер в алфавіті, тобто, ціле число. Таким чином, формується вектор-рядок:

$$\psi = \left\| \psi_j \right\|, \; j = 1, 2, 3. \tag{2}$$

Шифрування здійснюється шляхом множення на цей вектор ціло-чисельної матриці того ж порядку

$$A_n = \left\| a_{ij} \right\|, \; i, \; j = 1, 2, 3, \tag{3}$$

в результаті чого маємо

$$A_n \psi = \sum_{j=1}^{n=3} a_{ij} \psi_j = f_i, \; i = 1, 2, 3, \tag{4}$$

де f_i – також цілі числа. Знаючи ці числа і матрицю (3), «законний» одержувач може без похибки дешифрувати блок з чисел (2) за допомогою перемноження зворотної матриці на вектор-рядок f :

$$\psi = A_n^{-1} f,\ f = \left\| f_i \right\|. \tag{5}$$

Проте зі збільшенням n в (2) – (5), тривалість обчислень, пов'язаних з перемноженням елементів матриць різко зростає. Так, рішення системи лінійних алгебраїчних рівнянь за правилом Крамера з $n = 20$, де використовуються аналогічні перемноження, вимагає зовсім нереалістичних витрат машинного часу [2, с. 43-44]. Дійсно, фігурує порядок 10^7 років. Тому, з цієї точки зору, варіант $n \to \infty$ може здатися ірраціональним.

І, тим не менш, нехай у нас є вектор-рядок з великої кількості n, чисел, що розташовуються на відрізку $x \in [0, 1]$ з інтервалом $\Delta\xi$. Використовуючи в (4) позначення

$$a_{ij} = k_{ij} \Delta\xi,\ i,\ j = 1, 2, ..., n$$

(*де* k_{ij}, *на відміну від елементів матриці* a_{ij}, *не обов'язково цілі числа*), маємо наступне

$$A_n \psi = \sum_{j=1}^{n} k_{ij} \psi_j \Delta\xi = f_i,\ i = 1, 2, ..., n. \tag{6}$$

В разі $n \to \infty$, вектор Ψ та матриця A_n переходять в безперервні функції:

$$A\psi_n \to (A\psi)(x);\ k_{ij} \to k(x, \xi);\ \psi_j \to \psi(\xi);\ \Delta\xi \to d\xi;\ f_i \to f(x),$$

внаслідок чого система лінійних алгебраїчних рівнянь (6) перетворюється на інтегральне рівняння Фредгольма першого роду:

$$(A\psi)(x) = \int_0^1 k(x, \xi) \psi(\xi) d\xi = f(x),\ x \in [0, 1]. \tag{7}$$

Отже, якщо в (4) для перетворення початкового вектора Ψ до, т. з. «невпізнаного виду» f, ми мали $3 \times 3 = 9$ цілих чисел, то ядро $k(x, \xi)$, для реалізації тієї ж мети, має у своєму розпорядженні набір нескінченної кількості дійсних чисел. І, тим не менш, рівняння (7) є абсолютно особливий об'єкт, зокрема, з тієї причини, що його ядро не можна вибирати довільним. Справді, якщо, наприклад:

$$k(x, \xi) = k_0(\xi);\ k(x, \xi) = x k_1(\xi),$$

то, інтегруючи за формулою (7), отримуємо $f = b_0$ та $f = b_1 x$, де b_0, b_1 – відповідні константи. - Інакше кажучи, відбувається «знищення» інформації про функцію $\psi(x)$.

Щоб уникнути цього, а також для забезпечення єдності розв'язку рівняння (7), оскільки вихідний текст, який визначається функцією, однозначний, ядро має бути замкнутим. Останнє означає, що

$$\int_0^1 k(x, \xi) \varphi(\xi) d\xi = 0,\ x \in [0, 1]$$

лише в тому випадку, коли функція $\varphi(x) = 0$.

Множина відповідних в даному контексті ядер є практично необмеженою; їх можна, за загальним правилом, конструювати. Як приклад наведемо ядро

$$k(x, \xi) = \begin{cases} (1 - x)\xi,\ 0 \le \xi \le x; \\ x(1 - \xi),\ x \le \xi \le 1; \end{cases}$$

за допомогою нього, наприклад, для елементів (1) шифрування за формулою (7) проводиться в аналітичному вигляді, оскільки відповідні інтеграли є табличними. Справді, тут присутні інтеграли виду

$$\int_0^x \xi \sin \omega\xi d\xi = \frac{\sin \omega\xi}{\omega^2} - \frac{\xi \cos \omega\xi}{\omega} \Bigg|_0^x = \frac{\sin \omega x}{\omega^2} - \frac{x \cos \omega x}{\omega}.$$

Слід зауважити, якщо інтегральне рівняння (7) має кінцеве число різних рішень (*інакше кажучи, не є замкнутим*), то принципових ускладнень внаслідок цього також не виникає. Законному (*тобто легітимному*) одержувачу потрібно лише, додатково передати набір відповідних коефіцієнтів при власних функціях ядра $k(x, \xi)$.

Звертаючи увагу на особливості властивостей інтегрального рівняння (7), можна відзначити, що не знаючи структури оператора A (*в першу чергу, мається на увазі ядро* $k(x, \xi)$), визначення функції $\psi(x)$ є нездійсненним, навіть теоретично.

Традиційно рівняння такого типу розглядається в постановках теорії некоректних задач. При цьому рішення фактично знаходиться засобами обчислювального експерименту, що не придатне для автоматизованого алгоритму $f \to \Psi$. Іншими словами, образно висловлюючись: - біля кожного бухгалтера не можна посадити математика високої кваліфікації, діяльність якого, до того ж, може бути досить тривалою.

Спеціального виду моделювання обробки інформації процедурою інтегрування дозволяє позбутися від згаданого фактора некоректності, внаслідок чого алгоритм $f \to \Psi$ стає: по-перше, обчислювально стійким, а по-друге, – легко піддається формалізації (*тобто дешифруванню в автоматичному режимі*) [3].

3. Математична реалізація

У загальних рисах суть пропозиції, щодо вирішення відповідного інтегрального рівняння у аналітичному вигляді, прийнятному для процедури його обчислювання, розглянута нижче.

Відомо,що інтегральних операторів, за допомогою яких може здійснюватися шифрування $A\psi = f$, а потім дешифрування $\psi = A^{-1} f$, в аналітичному вигляді (*що дуже важливо*), є велика кількість. Наведемо відповідні приклади.

1. Шифрування:

$$(A\psi)(x) = \int_0^x \frac{\psi(\xi)\,d\xi}{x+\xi} = f(x) = \sum_{n=0}^{N} a_n x^n;$$

дешифрування, після розкладання $f(x)$ в степеневий ряд, інакше кажучи, формула обернення [4]:

$$\psi(x) = \sum_{n=0}^{N} \frac{a_n}{b_n} x^n,\ b_n = (-1)^n \left[\ln 2 + \sum_{m=1}^{n} \frac{(-1)^m}{m} \right].$$

2. Шифрування:

$(A\psi)(x) = \psi(x) - \int_\alpha^x g(x)h(\xi)\psi(\xi)\,d\xi = f(x),$ де як $g(x)$, так і $h(x)$ – довільні функції.

Дешифрування [4, с. 162]: $\psi(x) = f(x) + \int_\alpha^x R(x, \xi)\psi(\xi)d\xi,$

де $R(x, \xi) = g(x)h(\xi)\exp\left[\int_\xi^x g(\xi)h(\xi)\,d\xi\right].$

3. Шифрування:

$$(A\psi)(x) = \int_{-\infty}^{\infty} \frac{\psi(\xi)\,d\xi}{\xi - x} = f(x);$$

дешифрування [4, с. 193]:

$$\psi(x) = \frac{1}{\pi^2} \int_{-\infty}^{\infty} \frac{f(\xi)\,d\xi}{\xi - x},$$

де сингулярні інтеграли тлумачаться у сенсі головного значення по Коші.

При цьому слід мати на увазі наступні особливості:

- шифрування може проводитися шляхом послідовного застосування декількох інтегральних операторів (*аналогічно застосовуються формули обернення*);
- передбачається поділ масиву інформації на частини, з варіюванням операторів інтегрування, а також їх параметрів і функцій за спеціальною програмою;
- ця програма, включає реалізацію формул звернення, або ж алгоритми розв'язання інтегральних рівнянь, що функціонують у легітимного одержувача інформації в автоматичному режимі;
- власне процеси передачі повідомлень не розглядаються, в даному випадку, акцент робиться на тому, що вони хоч і розміщені в мережі, однак не є доступні для дешифрування без відповідного програмного забезпечення;
- в методологічному аспекті досягається спряженість з криптологією в її традиційному форматі, оскільки напрацьований апарат перестановок, підстановок та ін. може використовуватися і відносно сукупності елементів (1).

Розглянемо конкретний приклад шифрування і дешифрування в аналітичному вигляді для інтеграла [4]:

$$\int_0^x (ax - a\xi + c)\psi(\xi)\,d\xi = f(\xi), \tag{8}$$

де «*a*» та «*c*» – довільні константи. При цьому, законному одержувачу і, можливо, іншої не уповноваженої особі (*порушнику*) доступний зашифрований сигнал $f(x)$. Але, на відміну від порушника, технічні засоби легітимного одержувача мають в своєму складі програмну реалізацію вирішення інтегрального рівняння Вольтерра (8). Крім того, є велика вірогідність того, що сторонній одержувач, скоріш за все, не буде мати до неї доступу.

Відповідна програма автоматично здійснює перетворення $f(x) \to \Psi(x)$, тобто, робить дешифрування (*відновлення*) вихідної функції $\Psi(x)$. У програму також закладений алгоритм, згідно з яким можуть варіюватися параметри «*a*» і «*c*» на інтервалі [*0, x*].

Рішення інтегрального рівняння (8) має вигляд:

$$\psi(x) = \frac{1}{c}\frac{d}{dx}\left[\exp\left(-\frac{a}{c}x\right)\int_0^x \exp\left(\frac{a}{c}\xi\right)\frac{d}{d\xi} f(\xi)\,d\xi\right]\cdot \tag{9}$$

Нехай у (8) функція $\psi(x) = \sin\omega x$. Зокрема, це може бути буква, або символ (1), або ж член ряду Фур'є, що представляє функцію складного виду. Тоді зашифрована (*шляхом інтегрування (8)*) функція має вигляд

$$f(x) = \int_0^x (ax - a\xi + c)\sin\omega\xi\,d\xi = -\frac{ax}{\omega}\cos\omega\xi - a\left(\frac{\sin\omega\xi}{\omega^2} - \frac{\xi\cos\omega\xi}{\omega}\right) -$$

$$-\frac{c}{\omega}\cos\omega\xi\Big|_0^x = \frac{1}{\omega}(ax + c) - \frac{c}{\omega}\cos\omega x - \frac{a}{\omega^2}\sin\omega x, \tag{10}$$

відповідно в (9)

$$\frac{d}{d\xi} f(\xi) = \frac{a}{\omega} + c\sin\omega\xi - \frac{a}{\omega}\cos\omega\xi\cdot$$

Далі отримуємо в (9) інтеграл

$$\int_0^x \exp\left(\frac{a}{c}\xi\right)\left(\frac{a}{\omega} + c\sin\omega\xi - \frac{a}{\omega}\cos\omega\xi\right)d\xi = \frac{c}{\omega}e^{\frac{a}{c}\xi} +$$

$$+\frac{ce^{\frac{a}{c}\xi}}{\left(\frac{a}{c}\right)^2 + \omega^2}\left(\frac{a}{c}\sin\omega\xi - \omega\cos\omega\xi\right) - \frac{\frac{a}{\omega}e^{\frac{a}{c}\xi}}{\left(\frac{a}{c}\right)^2 + \omega^2}\left(\frac{a}{c}\cos\omega\xi +\right.$$

$$+\omega\sin\omega\xi)\Big|_0^x=\frac{c}{\omega}e^{\frac{a}{c}x}+\frac{ce^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\sin\omega x-\omega\cos\omega x\right)-$$

$$-\frac{\frac{a}{\omega}e^{\frac{a}{c}x}}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\cos\omega x+\omega\sin\omega x\right)-\frac{c}{\omega}-\frac{c(-\omega)}{\left(\frac{a}{c}\right)^2+\omega^2}+\frac{\frac{a}{\omega}\frac{a}{c}}{\left(\frac{a}{c}\right)^2+\omega^2}. \qquad (11)$$

В цьому виразі його три останні складові в результаті перетворень дорівнюють нулю, тобто:

$$-\frac{c}{\omega}-\frac{c(-\omega)}{\left(\frac{a}{c}\right)^2+\omega^2}+\frac{\frac{a}{\omega}\frac{a}{c}}{\left(\frac{a}{c}\right)^2+\omega^2}=-\frac{c}{\omega}+\frac{c^3\omega}{a^2+(c\omega)^2}+\frac{a^2c}{\omega\left[a^2+(c\omega)^2\right]}+$$

$$=\frac{-c\left[a^2+(c\omega)^2\right]+c^3\omega^2+a^2c}{\omega\left[a^2+(c\omega)^2\right]}=\frac{-ca^2-c^3\omega^2+c^3\omega^2+ca^2}{\omega\left[a^2+(c\omega)^2\right]}=0.$$

Множення частини, що залишилася у виразу (11) на експоненту $\exp\left(-\frac{a}{c}x\right)$, згідно (9), приводить до наступного:

$$\frac{c}{\omega}+\frac{c}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\sin\omega x-\omega\cos\omega x\right)-\frac{\frac{a}{\omega}}{\left(\frac{a}{c}\right)^2+\omega^2}\left(\frac{a}{c}\cos\omega x+\omega\sin\omega x\right)=$$

$$=-\frac{c^2}{a^2+(c\omega)^2}\frac{a^2+(c\omega)^2}{c\omega}\cos\omega x.$$

Скорочуючи в даному виразі множники, і після диференціювання згідно (9), відновлюємо функцію в її початковому вигляді: $\psi(x)=\sin\omega x$. Можна помітити, що вона зовсім не схожа на зашифроване повідомлення (10). Таким чином, за рахунок використання розглянутих пропозицій можна досягнути поставленої мети – забезпечення криптографічного шифрування даних, що представлені у формі неперервних однозначних функціональних залежностей, та їх наступне дешифрування, завдяки ефективного вирішення інтегральних рівнянь.

4 Висновки

В межах роботи кількох міжнародних конференцій [5-7] автори доповідали можливі варіанти практичної реалізації даного способу (криптографічних перетворень), крім того був запропонований варіант функціональної системи шифрування, та визначені орієнтовні терміни виготовлення дослідного зразку відповідної криптографічного системи [8]. Як виявилося за результатами проведення профільних наукових дискусій, створення відповідної системи є цілком можливим. Це, принаймні, буде паритетним рішенням по відношенню до потенційних "криптографічних" загроз з боку квантового комп'ютеру. Зрозуміло, що для коректної організації порівняльного експерименту потрібен зразок діючого квантового комп'ютеру, що й обумовлює зупинку досліджень в запропонованому авторами напрямі криптографії.

Посилання

[1] Средства обеспечения информационной безопасности в сетях передачи данных: задачи и методические указания / Составители: А. В. Крыжановский, Н. В. Киреева, В. В. Пугин. – Самара: Поволжская государственная академия телекоммуникаций и информатики, 2008. – 61 с.

[2] Форсайт Дж., Малькольм М. Моулер К. Машинные методы математических вычислений. – М.: Мир, 1980. – 280 с.
[3] Перчик Е. Методология синтеза знаний: преодоление фактора некорректности задач математического моделирования / www.pelbook.narod.ru (2-я ред.)
[4] Полянин А. Д., Манжиров А. В. Справочник по интегральным уравнениям. – М.: Физматлит, 2003. – 608 с.
[5] Громыко И.А. Криптография нового поколения с сопряжением дискрет / И. А. Громыко, К. О. Швагер // Матеріали V-ої Міжнародної НТК «Захист інформації і безпека інформаційних систем». Тез. Доп. – Львів: Вид-во Львівська політехніка. – 2016. – 172 с. – С.104-106. ResearchGate: www.researchgate.net/publication/301747721 - DOI: 10.13140/RG.2.1.3936.8567
[6] Громыко И.А. Постквантовая криптография в ракурсе общей парадигмы защиты информации // Материалы 5-й Международной НТК «Информационные системы и технологии. Харьков – Коблево. ИСТ-2016». Харьков – Коблево. Тезисы доклада. 12 страниц. - Индекс DOI: 10.13140/RG.2.2.29107.02.087.
[7] Громико І.О. Общая парадигма защиты информации в свете новой редакции (2011г.) Закона Украины «Про информацию» // Матеріали Міжнародної НП Інтернет–конференції «Інформаційна і економічна безпека (INFECO-2014).
[8] Громыко И.А. Криптография в общей парадигме защиты информации. Вариант выхода из квантового кризиса // Защита информации. INSIDE. –СпБ.: ООО «Издательский Дом «Афина» -№6 – 2016 г. – с. 48-56.

Reviewer: Volodymyr Maxymovych, Doctor of Sciences (Eng.), Full Prof., ICTA, Lviv Polytechnic National University, Bandera St., 12, Lviv, 79013, Ukraine. E-mail: vmax@polynet.lviv.ua

Received on Jule 2020.

Authors:

Mykhailo Suknov, Cand. Sc. (Education), Prof., Head of department, Kharkiv National University of Radio Electronics, Ukraine.
E-mail: mykhailo.suknov@nure.ua

Igor Gromyko, Ph.D. (Technical), Associate Professor, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: i.gromyko@karazin.ua

Eugene Perchik, Ph.D., Senior Research Officer, Joint Stock Company "STI TRR", Kharkiv, Ukraine.

Method of cryptologic data transformations.

Abstract. Countering a quantum computer in the process of illegal ultra-high-speed decryption of messages is technically feasible. Information owner must oppose the competitor's computer with tasks, the solution of which requires an infinite number of operations during decryption. For example, the dependence of functions on an infinite number of informative features. The owner encrypts by integrating the functions, the recipient decrypts by solving the integral equations. It is not a discrete but an analog approach that prevails here. The basis for the implementation of this approach was created by Polish scientists. Mathematician Stefan Banach (*1892-1945*), who created modern functional analysis, and Marian Mazur (*1909-1983*), the author of " The Qualitative Theory of Information". Their theory was created in contrast with the "Quantitative Information Theory". Cryptologists who have devoted their whole lives to improving the "discrete" theory and found themselves close to power (*and finance*), try not to recall that Claude Shannon in his basic work "Communication Theory of Secrecy Systems" more than once emphasized the discrete focus of his developments anticipating future research on the specific limitations of his work adapted to the communication theory. Forgetting about the unlimited speeds and amounts of memory of quantum computers the orthodox talk about redundancy and further purely technical issues, including administrative leverages for counteracting against opponents. It is impossible to stop the progress of science. Experiments have shown the reality of creating such post-quantum-level cryptographic systems.

Keywords: Cryptology; Quantum Computer; Automated encryption technologies and decryption.

Рецензент: Владимир Максимович, д.т.н., проф., Национальный университет «Львовская политехника», Львов, 79013 Украина. E-mail: vmax@polynet.lviv.ua

Поступила: Июль 2020.

Авторы:

Михайло Сукнов, к.т.н., проф., зав. каф., Харьковский национальный университет радиоэлектроники, 61166, Украина.
E-mail: kate7smith12@gmail.com

Игорь Громыко, к.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, 61022, Украина.
E-mail: i.gromyko@karazin.ua

Евгений Перчик, к.т.н., ст. научный сотрудник, АО НТИ ТТР, Харьков, Украина.

Способ криптологических преобразований данных.

Аннотация. Противодействие квантовому компьютеру в процессе неуполномоченной сверхскоростной расшифровки сообщений - технически осуществимо. Собственник информации должен противопоставить компьютеру конкурента задачи, решение которых потребует бесконечное число операций при дешифровке. Например, - зависимость функций от бесконечного числа информативных признаков. Собственник шифрует путем интегрирования функций, получатель дешифрует ре-

шением интегральных уравнений. В этом случае превалирует не дискретный, а аналоговый подход. Базис для реализации такого подхода создали польские учёные. Математик Стефан Банах (*Stefan Banach, 1892–1945*), создавший современный функциональный анализ и Мариан Мазур (*Marian Mazur, 1909-1983*) автор «Качественной теории информации». Их теория была создана в противовес «Количественной теории информации». Криптологи, которые всю жизнь посвятили совершенствованию «дискретной» теории и оказались приближенными к власти (*и финансам*), стараются не вспоминать, что Клод Шеннон в своей базовой работе «Теория связи в секретных системах» не единожды подчеркнул дискретную направленность своих разработок, предупредив будущих исследователей о специфической ограниченности своей работы, адаптированной под теорию связи. Забывая о неограниченных скоростях и объёмах памяти квантовых компьютеров, ортодоксы говорят про избыточность и прочие сугубо технические моменты, применяя в отношении своих оппонентов все возможные рычаги противодействия. Прогресс науки остановить невозможно. Исследования показали реальность создания подобных криптографических систем постквантового уровня.

Ключевые слова: криптология; квантовый компьютер; технологии автоматизированного шифрования и дешифрования.