МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 17-20 липня 2023 р.

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2023)

Odesa, Ukraine, July 17-20, 2023

Conference Proceedings

Odesa

2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2023)

Одеса, Україна, 17-20 липня 2023 р.

Матеріали конференції

Одеса
2023

ЗМІСТ

СЕКЦІЯ 2. КІБЕРБЕЗПЕКА ТА КІБЕРПСИХОЛОГІЯ

УДК 004.725.5

Григор'єва Т.І., кандидат технічних наук, доцент,
Міжнародний гуманітарний університет, місто Одеса
tig15090808@gmail.com
Йона Л.Г., кандидат технічних наук, доцент,
Міжнародний гуманітарний університет, місто Одеса
yonalarisa66@gmail.com
Мазур Г.Д.
Міжнародний гуманітарний університет, місто Одеса
Anna2102@i.ua
Кравченко І.А.
Міжнародний гуманітарний університет, місто Одеса
irakravchenko609@gmail.com

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ШЛЯХОМ ШИФРУВАННЯ НА ОСНОВІ ТЕНЗОРНИХ МЕТОДІВ

Анотація. *Для забезпечення захисту основних властивостей інформації, а саме конфіденційності, цілісності та доступності, а також для прискорення процесу шифрування, з ціллю підвищення ефективності засобів захисту конфіденційної інформації, пропонується здійснювати шифрування повідомлення за допомогою операцій тензорного аналізу.*

У сучасному світі інформаційних технологій, при обміні документами по незахищених каналах зв'язку, користувачі можуть зіткнутися з проблемою витоку інформації чи її модифікування. Зловмисники можуть завдати істотних збитків банківським та комерційним структурам, державним підприємствам та організаціям, а також приватним особам, які використовують електронний документообіг. Для того, щоб вирішити цю проблему, необхідно забезпечити захист інформації, що міститься в документі та провести процедуру встановлення автентичності автора і самого документа.

Комплекс процесів та технологічних рішень, які допомагають здійснити захист даних та запобігання несанкціонованому доступу до системи, входять до складу понять, що визначають кібербезпеку, яка є одним із найважливіших елементів національної і інформаційної безпеки [1,2].

Застосування тензорних методів в технічних напрямках, в тому числі, в телекомунікаціях [3-10], отримані результати виводять дослідження на новий рівень, який не вдавалося отримати, використовуючи методи, що застосовувалися раніше. Використання тензорного аналізу запропоновано для дослідження характеристик якості мережі масового обслуговування, яка складається з систем масового обслуговування M/M/1 [4]. Обґрунтовано доцільність тензорного методу, що дозволяє отримувати ефективні рішення оцінки характеристик якості при одночасному аналізі мережі та мережі масового обслуговування різної структури та розмірів функціональних характеристик [4,8].

Тензорні методи дозволяють розв'язувати різні мережеві завдання, прогнозувати стан мережі на певному проміжку часу з урахуванням топології мережі та особливості функціонування використовуваних протоколів. Показано можливість спільного математичного моделювання структурних властивостей та функціональних характеристик телекомунікаційних систем за допомогою спеціального способу завдання системи координат

та властивості інваріантності тензора, де інваріантом є значення трафіку у кожний конкретний момент часу [3-5].

В [6] розглянуто тензорну модель телекомунікаційної мережі, яку представлено в базисі міжполюсних шляхів і внутрішніх вузлових пар. Перевагою використання саме тензорної моделі є забезпечення якості обслуговування за показниками пропускної здатності, середньої міжкінцевої затримки та ймовірності втрат пакетів.

Для дослідження якісних характеристик функціонування мережі MVNO/LTE запропоновано тензорний метод декомпозиції архітектури мережі з метою отримання оптимальної конфігурації з'єднання базових станцій e-NodeB за критеріями максимальної пропускної здатності та заданих параметрів затримки [8].

В задачах апроксимації випадкових процесів та полів, при відновленні дискретизованих сигналів пропонується використовувати тензорні сплайни [9,10].

На данний час теорія кодування [11-14] дуже добре розвивається і застосовує різноманітні розділи вищої математики: теорія ймовірностей, теорія чисел, математична логіка, такі розділи лінійної алгебри, як матриці, векторна алгебра і теорія поліномів.

Забезпечити захист основних властивостей інформації, а саме конфіденційності, цілісності та доступності, можна шляхом використання криптографічних алгоритмів. Якщо йдеться про забезпечення конфіденційності, тобто захисту від витоку інформації, то це вирішується шляхом шифрування відкритого повідомлення. Зашифроване повідомлення у вигляді криптограми передається одержувачеві по незахищеному каналу. При цьому, для зашифровування та розшифрування повідомлення, необхідно знати ключ шифрування (правило перетворення) [15].

В залежності від обраного алгоритму шифрування, операції зашифровування та розшифрування можуть виконуватися по-різному. Так, якщо використовувати симетричний алгоритм шифрування, то процедури зашифровування та розшифровування виконуватимуться одним спільним секретним ключем.

В разі використання асиметричного алгоритму, процес шифрування буде виконуватися двома різними ключами. Тобто зашифровування тексту буде здійснюватися відправником за допомогою відкритого ключа, а процес відновлення повідомлення з криптограми – за допомогою іншого секретного ключа одержувача. Ця пара ключів обирається за певним законом [16].

Проте, для процесу шифрування частіше обирають саме симетричні системи зі спільним секретним ключем. Цей вибір пояснюється швидкістю шифрування (асиметричні системи працюють повільніше).

Для підвищення ефективності засобів захисту конфіденційної інформації пропонується здійснювати шифрування повідомлення тензорними методами [17,18].

Розглянемо початковий вихідний текст, наприклад, у вигляді тензора четвертої валентності T_{ijk}^{h} n – мірного простору, $h,i,j,k=\overline{1,n}$. Якщо здійснити алгебраїчне додавання з числовим коефіцієнтом 0,5 після операцій симетрування і альтернування по двох коваріантних індексах, то компоненти вихідного тензора не зміняться [17]:

$$T_{ijk}^{h}=0{,}5(T_{(ij)k}^{h}+T_{[ij]k}^{h}), \qquad (1)$$

де формулою $T_{(ij)k}^{h}=T_{ijk}^{h}+T_{jik}^{h}$ задається операція симетрування по двох індексах і та j; $T_{[ij]k}^{h}=T_{ijk}^{h}-T_{jik}^{h}$ – операція альтернування по індексах і та j.

Перетворення (1) може виступати в якості ключа шифрування. В результаті операцій симетрування і альтернування по двох індексах із вихідного тензора T_{ijk}^{h} ми отримаємо два тензори $T_{(ij)k}^{h}$ і $T_{[ij]k}^{h}$, які можно зберігати або відправляти. Тобто в процесі шифрування із одного тензора ми отримали два тензори. Потім за допомогою формули (1) можна здійснити розшифрування. Оскільки розглянуті операції симетрування і альтернування є дуже

простими, то всі обчислення не потрибують затрати великих ресурсів. Тому процеси шифрування і розшифрування є простими і достатньо швидкими, тобто є ефективними.

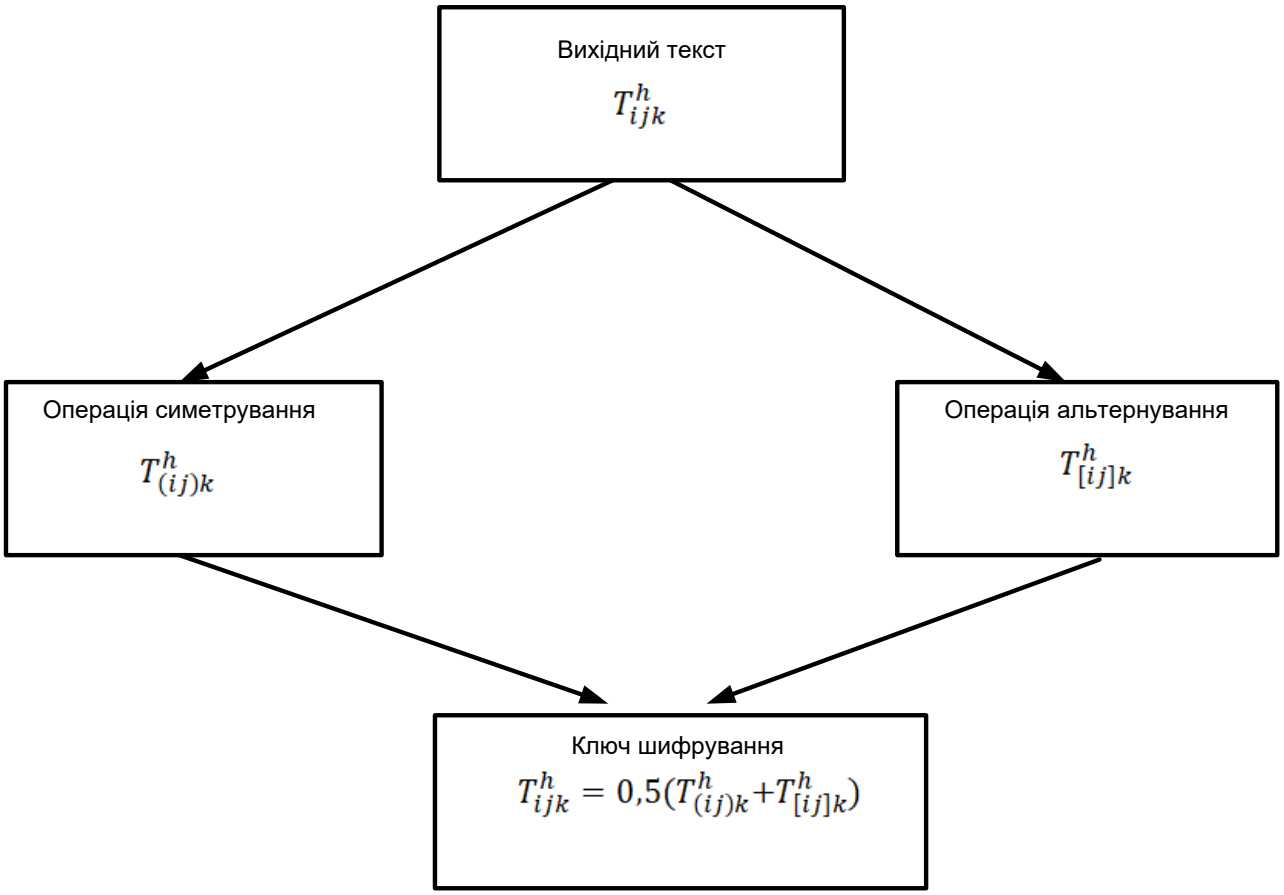

Рисунок 1. Процес створення ключа шифрування

Таким чином, можна зробити висновки, що за результатом виконання операцій тензорного аналізу, можна отримати можливість зашифровування повідомлень та розшифровування криптограм. При цьому відбувається підвищення швидкодії процесу забезпечення захисту конфіденційної інформації при здійсненні документообігу.

Література

1. Kivalov S. Detection and prediction of DDoS cyber attacks using spline functions/ S. Kivalov, I. Strelkovskaya // IEEE TCSET 2022, 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – 2022.

2. Горлинський В. Кібербезпека як складова інформаційної безпеки України / Віктор Горлинський, Борис Горлинський // Information Technology and Security. – 2019. – Vol. 7, Iss. 2 (13). – P. 136-148.

3. Поповський В. В. Основи теорії телекомунікаційних систем: підручник. – Харків: ХНУРЕ, 2018. – 368с.

4. Tensor method of traffic management problems solving with service quality network parameters maintenance [Text] / I.V. Strelkovskaya, I.N. Solovskaya // Eastern-European Journal of Enterprise Technologies. – 2011. – V. 5, № 3(53) – P. 37-42.

5. Тензорный метод оценки максимальной пакетной очереди узловой сети [Текст] / И.В. Стрелковская, И.Н. Соловская // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЭ, 2010. – № 163. – С. 7-12.

6. Лемешко О. В. Дослідження вдосконаленої тензорної моделі маршрутизації в телекомунікаційній мережі, представленої в базисі міжполюсних шляхів і внутрішніх вузлових пар/ О. В. Лемешко, М. О. Євдокименко // Проблеми телекомунікацій. - 2020. – 1(26). – С. 3-22.

7. Strelkovskaya I.V. LTE/MVNO networks structure optimization based on tensor decomposition [Text] / I.V. Strelkovskaya, I.N. Solovskaya // Information and telecommunication sciences. – July-December – 2014. – V. 5, № 2(9). – P. 14-20.

8. Strelkovskaya I.V. Tensor model of multiservice network with different classes of traffic service/ I.V. Strelkovskaya, I.N. Solovskaya// Radioelectron.Commun.Syst – 2013. – 56, 296–303. https://doi.org/10.3103/S0735272713060058.

9. Стрелковская И.В. Тензорные сплайны в задачах восстановления дискретизированных случайных процессов и полей [Текст] / И.В. Стрелковская, Т.И. Григорьева // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЭ, 2007. – Вып. 151. – С. 65-69.

10. Стрелковская И.В. Сплайн-матрицы в процедуре рекурсивной оценки состояний сетевых элементов и их режимов [Текст] / Стрелковская И.В., Григорьева Т.И. // Комп'ютерні технології друкарства: Збірник наукових праць. – Львів, 2011. – №25. – С. 84-92

11. Білинський Й. Й. Електронні системи: навчальний посібник / Й. Й. Білинський, К. В. Огороднік, М. Й. Юкиш. – Вінниця: ВНТУ, 2011. – 208 с.

12. Романюк М.І. Основи теорії інформації та кодування. Конспект лекцій / М.І. Романюк, Ю. Г. Савченко// КПІ ім. Ігоря Сікорського. – Електронні текстові данні – Київ: КПІ ім. Ігоря Сікорського, 2019. –70 с.

13. Krasnobaev V. Mathematical Model of the Process of Tabular's Implementation of the Operation Algebraic Multiplication in the Residues Class/ V. Krasnobaev, M. Zub M, T. Kuznetsova, I. Perevozova, O. Maliy // 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – 2019. – P. 1-6.

14. Краснобаєв Віктор. Метод виконання операції додавання двох залишків за модулем/ Віктор Краснобаєв, Михайло Багмут, Єлизавета Лазарєва, Людмила Горбачова, Катерина Кузнецова // IV Міжнародна науково-практична конференція "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS)" 15 - 16 квітня 2021р.: тези доп. – Київ, Україна. – 2021. – С. 70-71.

15. Йона Л.Г. Криптографічний захист електронного документообігу [Текст] / Л. Г. Йона, О. О. Йона, В. С. Терешко // Цифрові технології.–2013. – № 13. – С. 142–146.

16. Hellman M.E. The Mathematics of Public-Key Cryptography / August 1979 Scientific American, INC, 1979. P. 146-157.

17. Разумова М. А., Хотяїнцев В. М. Основи векторного і тензорного аналізу. — К. : ВПЦ «Київський університет», 2011. – 216 с.

18. De Souza Sánchez Filho E. Tensor Calculus for Engineers and Physicists. — Springer, 2016. – 374 p.