Lecture Notes in Networks and Systems 809

Stanislav Dovgyi
Oleksandr Trofymchuk
Vasyl Ustimenko
Larysa Globa *Editors*

Information and Communication Technologies and Sustainable Development

Advanced Approaches and Innovations in Up-to-Date Networks and Systems

Springer

Lecture Notes in Networks and Systems 809

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the worldwide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Stanislav Dovgyi · Oleksandr Trofymchuk ·
Vasyl Ustimenko · Larysa Globa
Editors

Information and Communication Technologies and Sustainable Development

Advanced Approaches and Innovations in Up-to-Date Networks and Systems

Springer

Editors
Stanislav Dovgyi
Institute of Telecommunications and Global Information Space of NAS of Ukraine
Kyiv, Ukraine

Oleksandr Trofymchuk
Institute of Telecommunications and Global Information Space of NAS of Ukraine
Kyiv, Ukraine

Vasyl Ustimenko
Institute of Telecommunications and Global Information Space of NAS of Ukraine
Kyiv, Ukraine

Larysa Globa
"Igor Sikorsky Kyiv Polytechnic Institute"
National Technical University of Ukraine
Kyiv, Ukraine

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-46879-7 ISBN 978-3-031-46880-3 (eBook)
https://doi.org/10.1007/978-3-031-46880-3

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Tenzor Methods in Cyber Security

Tetyana Grygoryeva(✉), Larysa Yona, and Anna Mazur

International Humanitarian University, Fontanskaya Road Str. 33, Odesa 65009, Ukraine
tig15090808@gmail.com, anna2102@i.ua

Abstract. The development of information technology and intensive use of the Internet has revealed problems related to information security. The issues of protecting information transmitted through communication channels and requiring long-term storage become relevant; the need for authentication procedures for users and messages; improving system performance and reliability. Various tasks of modern information security are solved with the help of cryptographic protocols. Various sections of higher mathematics are successfully used in information protection tasks. In this article to increase the effectiveness of information protection means, it is proposed to use such a mathematical apparatus as tensor analysis. The possibility of using tensor methods in solving various problems of cryptographic protection of information is shown. As a result of tensor analysis operations, this article shows the possibility of encrypting messages and decrypting cryptograms. The possibility of using tensor analysis in the construction of hash functions is shown additionally. In order to increase the effectiveness of means of protecting confidential information, it is proposed to encrypt messages using tensor analysis operations. At the same time, there is an increase in the speed of the process of ensuring the protection of confidential information in the implementation of document flow.

Keywords: Cyber Security · Cryptographic Protection · Encryption Key · Tensor Methods · Hash Function

1 Introduction

The formation of the fourth-generation of mobile communication network and, in the near future, the transition to the networks of the fifth and subsequent generations, combined with the ubiquitous accessibility of smartphones, that contributes to the emergence and development of the concept of the "state in a smartphone", which is embodied in our life by the Ministry of Digital Transformation of Ukraine. The protection of personal data, at the same time, is the priority among all the tasks in the field of Cyber Security. Cyber protection of the state critical infrastructure is also extremely relevant. A separate important area that absolutely needs constant improvement is the system of cryptocoding of military telecommunications of all levels and state special telecommunications. Therefore, a very important task facing the professional education system is to improve the quality of specialist training to ensure Cyber Security and further development of the Ukrainian Cyber Security industry.

S. Dovgyi et al. (Eds.): ICT&SD 2022, LNNS 809, pp. 291–299, 2023.
https://doi.org/10.1007/978-3-031-46880-3_18

A set of processes and technological solutions that help protect data and prevent unauthorized access to the system is part of the concepts defining cyber security, which is one of the most important elements of national and information security [1, 2].

Various tasks of modern information protection are solved with the help of cryptographic protocols. Thus, protection of information confidentiality is carried out by converting an open message with encryption algorithms; confirmation of the authenticity of the user or document takes place with the help of authentication protocols; protection against interception of keys by an attacker is solved by key distribution protocols.

It should be remembered that cryptographic protocols are based on mathematical transformations. At the beginning of the era of computer networks, when the need for information protection arose, the mathematical methods used for cryptographic transformations were limited by the speed and cost parameters of the systems. Therefore, developers of cryptosystems were forced to reduce the reliability of data protection, giving priority to the speed parameter. That is why modern cryptocoding algorithms represent a compromise between the parameters of cryptoresistance, the cost of implementing the algorithm, and the speed of its operation. As computer systems have been developed, the speed increases and costs decrease in general, it has become possible to improve the level of data protection, due to the use of more complex mathematical tools.

The development of Cyber Security should move into the direction of increasing the security of information against unauthorized access. To solve this problem, it is very important to develop and improve Cryptocoding Methods. Based on this, along with the existing mathematical principles that are being established at the moment, when building new cryptocoding algorithms or improving existing ones, the use of Tensor Analysis is proposed.

2 Tenzor Methods in Telecommunication Systems

As practice has shown, the application of Tensor Methods in Science areas, including in Telecommunications [2–10], the obtained results are bringing the research to a new level, which could not be obtained using the earlier methods.

Usage of tensor analysis to research queueing network quality characteristics that consists of queueing systems M/M/1 was proposed. Appropriateness of tensor method allowing to get effective solutions of quality characteristics valuations under simultaneous analyses of network and queueing network of different structures a sizes functional characteristics was grounded [4].

Tensor methods allow solving various network tasks, forecasting the state of the network over a certain period of time, taking into account the network topology and the peculiarities of the functioning of the protocols used. The possibility of joint mathematical modeling of structural properties and functional characteristics of telecommunication systems using a special method of tasking the coordinate system and the invariance property of the tensor, where the invariant is the traffic value at each specific moment of time, is shown [3–5].

In [6], the tensor model of the telecommunication network is considered, which is presented in the basis of interpolar paths and internal node pairs. The advantage of using the tensor model is to ensure the quality of service conditions in terms of bandwidth, average end-to-end delay, and packet loss probability.

To research quality characteristics of MVNO/LTE network functioning was proposed the decomposition tensor method of network architecture in order to obtain optimal configuration of e-NodeB base stations connection according to the criteria of maximum throughput and given parameters of delay [7].

In problems of approximation of random processes and fields, it is suggested to use tensor splines when restoring discretized signals [9, 10].

3 Cryptographic Protection Problems

Currently, Coding Theory [11–14] has being developed extensively and various sections of Higher Mathematics are applied: Probability Theory, Number Theory, Mathematical Logic, and such sections of Linear Algebra as Matrices, Vector Algebra and Polynomial Theory.

In addition, the research in the field of information protection has led to the modeling of an Information Security Management System (ISMS (CMS)) for Information Systems (IS) and the formulation of initial requirements for an IS ISMS. Thus, in the work [15], the analogy of the display of ISMS for Information Systems in the form of Queuing System (QS) was established. This became possible due to the identification of structural and functional analogies between Information Security Management Systems and Queuing System. It was determined that the ISMS can be interpreted as a single-phase quasi-state with possible losses. Due to structural, meaningful and functional analogies, the newly created models allow to form a range of quantitative ISMS characteristics for IS. This makes it possible to ensure the effectiveness of the design process of Information Security Management Systems, taking into account the prospects of increasing complexity and the number of destructive effects on the information system by attackers. Computational experiments conducted using a specially developed software application confirmed the validity of the main theoretical propositions and practical developments.

This article proposes the use of Tensor Analysis to improve the effectiveness of information protection tools. So, for example, such actions on tensors as symmetrization and cycling specify the basic operations of permutation (P) and functional transformations (F) during encryption. The compression operation can be performed if the Tensor Analysis operation, namely convolution, is used as a hash function. With the help of tensor methods, it is possible to increase the size of the value of the hash function, which will increase the resistance of the hash function to collisions. Thus, the use of tensor analysis is possible in various tasks of cryptographic protection of information.

To ensure the protection of the main properties of information, namely confidentiality, integrity and availability, as well as to speed up the encryption process, with the aim of increasing the effectiveness of means of protecting confidential information, it is proposed to encrypt the message using tensor analysis operations.

In the modern world of information technologies, when exchanging documents over unsecured communication channels, users may face the problem of information leakage or its modification. Criminals can cause significant damage to banking and commercial structures, state enterprises and organizations, as well as private individuals who use electronic document management. In order to solve this problem, it is necessary to ensure the protection of the information contained in the document and implement a procedure for establishing the authenticity of the author and the document itself.

It is possible to ensure the protection of information by using cryptographic algorithms. If it is about ensuring confidentiality, that is, protection against information leakage, then this is solved by encrypting the open message. An encrypted message in the form of a cryptogram is transmitted to the recipient over an unsecured channel. At the same time, to encrypt and decrypt a message, it is necessary to know the encryption key (transformation rule) [16].

Depending on the chosen encryption algorithm, encryption and decryption operations can be performed differently. Thus, if you use a symmetric encryption algorithm, the encryption and decryption procedures will be performed with one common secret key.

In the case of using an asymmetric algorithm, the encryption process will be performed with two different keys. That is, the encryption of the text will be carried out by the sender with the help of a public key, and the process of restoring the message from the cryptogram - with the help of another secret key of the recipient. This pair of keys is chosen according to a certain law [17].

The features of cryptotransformations in asymmetric cryptosystems are:

- Direct cryptographic transformation is performed using the public key K_1;
- The reverse cryptographic transformation is performed using the private key K_2;
- The key pair (K_1, K_2) must be random and selected from the full set of key pairs allowed for use, and $K_1 \neq K_2$.

Cryptosystems combining both types of cryptographic systems are called hybrid, as a rule, the text of the message is encrypted using a symmetric cryptosystem, and the secret key is encrypted using an asymmetric cryptosystem.

However, symmetric systems with a shared secret key are more often chosen for the encryption process. This choice is explained by the speed of encryption (asymmetric systems work more slowly).

4 The Process of Creation the Encryption Key Using Tensor Methods

To increase the speed of means of protecting confidential information, it is suggested to encrypt the message using tensor methods.

Consider the initial source text, for example, in the form of a tensor of the fourth rank S^h_{ijk} of n – dimensional space, $h, i, j, k = \overline{1, n}$. If you carry out an algebraic addition with a numerical coefficient of 0.5 after the operations of symmetrization and antisymmetrization by two covariant indices, the components of the original tensor will not change [18, 19]:

$$S^h_{ijk} = 0,5(S^h_{(ij)k} + S^h_{[ij]k}) \tag{1}$$

where the formulas $S^h_{(ij)k} = S^h_{ijk} + S^h_{jik}$ and $S^h_{[ij]k} = S^{\ h}_{ijk} - S^h_{jik}$ define the symmetrization and antisymmetrization operations on two indices i and j. The Transformation (1) can act as an encryption key (Fig. 1).

As a result of the symmetrization and antisymmetrization operations on two indices from the original tensor S^h_{ijk}, we will get two tensors $S^h_{(ij)k}$ and $S^h_{[ij]k}$, which can be stored or sent. That is, in the encryption process, we obtained two tensors from one tensor. Then, with the help of formula (1), you can perform decryption.

Since the considered symmetrization and antisymmetrization operations are very simple, all calculations do not require the expenditure of large resources, so the encryption process is accelerated.

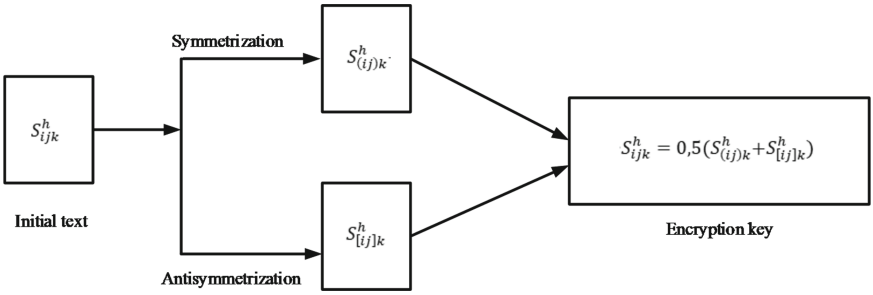

Fig. 1. The process of creation the encryption key.

Thus, it can be concluded that, based on the results of tensor analysis operations, it is possible to encrypt messages and decrypt cryptograms. At the same time, the speed of the process of ensuring the protection of confidential information during document circulation is increased.

5 Electronic Signature and the Procedure of Hashing

The second relevant method of information protection is the document authentication procedure, that is, the procedure for confirming the authenticity of a message during electronic document circulation and protecting electronic transactions during acquiring [20].

One of the most common methods of protecting electronic documents from copying, modification and forgery is the use of an electronic digital signature. There are special programs with the use of electronic signature (ES), which confirm the authenticity of the document, its details and the fact that this document was signed by a specific person.

The program of electronic document circulation using ES is currently being actively implemented in the State Institutions, which significantly expands the possibilities of using ES and the development of electronic document circulation in Ukraine.

These problems became especially relevant with the adoption of fundamental laws on information protection in many States at the international level, including Ukraine. In order to implement these laws, a public key infrastructure is being created in Ukraine, primarily to support the electronic signature system. At the same time, the primary task in Ukraine that requires a solution is the provision of services to the state authorities, local governments, legal entities and individuals to ensure the integrity, authenticity,

irrefutability, and in most cases, the confidentiality of information and various data provided in electronic form, electronic documents and messages, and software used by them. In addition, Ukraine has been integrating into the global information space, and its orientation towards the accession to the European Community prioritizes the task of ensuring the interaction of state authorities, local self-government, legal and physical people at the global level, using foreign and international information and information and communication systems, various information technologies, open Internet systems.

An electronic signature is data added to information, calculated using cryptographic transformation of protected information, as well as parameters, the presence of which makes it possible to be sure of its integrity and authenticity. An integral and essential part of ES is the use of hash functions [21].

One of the most important characteristics of hash functions, which led to their wide implementation in information protection systems, is the ability to obtain a long-length hash code from open text, which is much shorter than the message itself. This property eliminates plaintext redundancy and speeds up computation, thus increasing channel bandwidth and effectively reducing network traffic. Also, hash functions can be used to solve many other issues, for example, to hash user passwords in order to further encrypt them and store them in a database, or as a cryptographic checksum of a document (change detection code), or to check the integrity of a message.

In order to verify the integrity of the document and the impossibility of renouncing the authorship of the document during document circulation, there are technologies for applying various digital signature algorithms. However, regardless of the chosen algorithm of the ES, the formation of the electronic signature of each user is carried out using the procedure of hashing the open message in order to compress it and using a separate pair of keys (secret and open) to perform the procedures of setting and verifying the signature, respectively.

At the same time, the hash function itself is not part of the digital signature algorithm, but is a separate cryptographic algorithm [21, 22].

The sender of the message signs the document by performing the following actions:

– First, the message is compressed using a hash function;
– Then it forms a signature by transforming the hash code with a secret key.

The result of the conversion, i.e. the generated signature, is transmitted to the recipient along with the open message over an unsecured channel.

The recipient, having received an open document and a signature generated from this document, has to perform the following actions to verify its authenticity:

– restore the value of the hash code by applying the cryptographic transformation of the signature using the public key;
– compress the received open message with the same hash function to calculate the hash code value of the message;
– compare the received values of hash codes.

If both values match, the recipient recognizes the authenticity of the signature and the document.

Cryptographic algorithms usually use standardized hash functions [23], but this paper proposes a new method for creating hash functions. Below in the work we show the possibility of constructing hash functions using tensor analysis [18, 19].

Consider the use of hash functions for one-way cryptographic transformation, for example in order to confirm the authenticity of the original message.

6 Hash Function Construction Using Tensor Methods

It is proposed to construct a hash function (Fig. 2) using such tensor operations as simmetrization on three indices and convolution on two indices.

First, if to the original tensor of the fourth rank S^h_{ijk} of n – dimensional space, the symmetrization on three covariant indices i, j and k is applied:

$$S^h_{(ijk)} = S^h_{ijk} + S^h_{jki} + S^h_{kij} = S^h_{abc} \tag{2}$$

where $h, i, j, k, a, b, c = \overline{1, n}$, n is the dimension of the tensor space, we will get a new tensor of the same rank S^h_{abc}, which can be considered the result of the hash function or some other operations can be applied to it to reduce or increase its size.

Transformation (2) performs permutation (P) and functional transformations (F), which are basic transformations in encryption algorithms.

Secondly, if, after symmetrization on three indices to the tensor S^h_{abc}, we perform a convolution on the contravariant index h and on one of the covariant indices (for example, take the index a), then as a result we will get a tensor of the second rank, that is, the rank of the initial tensor decreases:

$$S_{bc} = S^{\alpha}_{\alpha bc} \tag{3}$$

where α is the dummy index, α = 1,2,…,n.

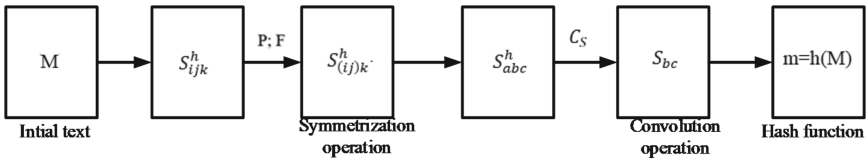

Fig. 2. Hash function construction.

Thus, the compression operation C_S (3) was performed, where the tensor analysis operation, namely convolution, was used as a hash function.

If we consider the operation of finding the product of two tensors, for example, the result of symmetrization on three indices and convolution S_{bc} – the tensor of the second rank and the initial tensor S^h_{ijk} of the fourth rank, then as a result we will get the tensor of the sixth rank, that is, we will increase the size of the value of the hash function, therefore the stability of the hash function will increase to collisions.

Therefore, it has been proven that the use of tensor methods for constructing hash functions for document authentication is expedient.

7 Conclusions

At the end of all considerations, we can draw the conclusions:

1. The use of tensor analysis is suitable for solving various problems of cryptographic information protection.
2. The possibility of using tensor analysis when constructing hash functions is shown.
3. In order to improve the effectiveness of means of protecting confidential information, the encryption of the message using tensor analysis operations is proposed.

References

1. Horlynskyi, V., Horlynskyi, B.: Cyber security as a component of information security of Ukraine. Inf. Technol. Secur. **2**(13), 136–148 (2019)
2. Kivalov, S., Strelkovskaya, I.: Detection and prediction of DDoS cyber attacks using spline functions. In: IEEE TCSET 2022, 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) (2022)
3. Popovskyi, V.V.: Fundamentals of the theory of telecommunication systems. Khnure, Kharkiv (2018)
4. Strelkovskaya, I.V., Solovskaya, I.N.: Tensor method of traffic management problems solving with service quality network parameters maintenance. East-Eur. J. Enterp. Technol. **3**(53), 37–42 (2011)
5. Strelkovskaya, I.V., Solovskaya, I.N.: Tensor method for estimating the maximum packet queue of a node network. Radiotechnique. Vseukr. interdisciplinary scientific and technical Sat. - Kharkiv: Khnure, no. **163**, 7–12 (2010)
6. Lemeshko, O.V., Yevdokymenko, M.O.: Study of the improved tensor model of routing in the telecommunications network, represented in the basis of interpolar paths and internal node pairs. Probl. Telecommun. **1**(26), 3–22 (2020)
7. Strelkovskaya, I.V., Solovskaya, I.N.: LTE/MVNO networks structure optimization based on tensor decomposition. Inf. Telecommun. Sci. **2**(9), 14–20 (2014)
8. Strelkovskaya, I.V., Solovskaya, I.N.: Tensor model of multiservice network with different classes of traffic service. Radioelectron. Commun. Syst. **56**, 296–303 (2013). https://doi.org/10.3103/S0735272713060058
9. Strelkovskaya, I.V., Grigoryeva, T.I.: Tensor splines in recovery problems of discretized random processes and fields. Radio technology: Vseukr. interdisciplinary scientific and technical Sat. - Kharkiv: Khnure Issue **151**, 65–69 (2007)
10. Strelkovskaya, I.V., Grigoryeva, T.I.: Spline-matrices in the procedure of recursive estimation of network elements and their regimes. Computer technologies of printing: Collection of scientific papers. Lviv no. **25**, 84–92 (2011)
11. Bilynsky, Y.Y., Ogorodnik, K.V., Yukysh, M.Y.: Electronic systems. Study guide. VNTU, Vinnytsa (2011)
12. Romaniuk, M.I., Savchenko, Y.G.: Basics of information theory and coding. Synopsis of lectures. KPI named after Igor Sikorsky. Electronic text data Sikorskyi, Kyiv (2019)
13. Krasnobayev, V., Zub, M., Kuznetsova, T., Perevozova, I., Maliy, O.: Mathematical model of the process of tabular's implementation of the operation algebraic multiplication in the residues class. In: International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), pp. 1–6 (2019)

14. Krasnobayev, V., Bagmut, M., Lazareva, Y., Horbachova, L., Kuznetsova, K.: The method of performing the operation of adding two remainders by modulo. In: IV International Scientific and Practical Conference "Problems of Cyber Security of Information and Telecommunication Systems (PCSITS)" 2021, pp. 70–71, Kyiv, Ukraine (2021)
15. Dranova, A., et al.: Methodology forming for the approaches to the cyber security of information systems management. J. Theor. Appl. Inf. Technol. **12**, 1993–2005 (2020)
16. Yona, L.G., Yona, O.O., Tereshko, V.S.: Cryptographic protection of electronic document circulation. Digital Technol. **13**, 142–146 (2013)
17. Hellman, M.E.: The Mathematics of Public-Key Cryptography. Scientific American INC, 146–157 (1979)
18. Razumova, M.A., Khotyaintsev, V.M.: Fundamentals of vector and tensor analysis. VOC "Kyiv University 216 (2011)
19. De Souza Sánchez Filho, E.: Tensor Calculus for Engineers and Physicists, p. 374. Springer (2016)
20. Yona, L.G., Kuehne, O.O.: Analysis of current protocols for cryptographic protection of electronic transactions. Digital Technol. **1**, 96–102 (2017)
21. Yona, L.G., Onatskyi, O.V., Belova, Y.V.: Banking security systems: training manual. SUITT, Odesa (2022)
22. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
23. Yevseiev, S.P., Yokhov, O.Y., Korol, O.G.: Data hashing in information systems. A monograph. Khneu, Kh. (2013)