Modeling of a cryptographic network based on application of CET-operations*

Volodymyr Rudnytskyi[1,2,†], Vira Babenko[2,*,†], Nataliia Lada[1,†], Tetiana Stabetska[3,†], Dmytro Pidlasyi[2,†] and Liubomyr Parkhuts[4,†]

[1] State Scientific Research Institute of Armament and Military Equipment Testing and Certification, Cherkasy, Ukraine
[2] Cherkasy State Technological University, 460 Shevchenko ave., 18006 Cherkasy, Ukraine
[3] The Bohdan Khmelnytsky National University of Cherkasy, 81 Shevchenko ave., 18031 Cherkasy, Ukraine
[4] Lviv Polytechnik National Universiti, 12 Stepan Bander str., 79013 Lviv, Ukraine

Abstract

The main purpose of this research is the development of principles applicable to modeling of cryptographic network with the defined architecture, as well as the definition of CET-operations sets to ensure the correct functionality of this network. We have defined and fulfilled several objectives to achieve the tasks mentioned above. As the first step, we have analyzed the attributes of cryptographic data security in computer networks. Next, we have analyzed the characteristics of utilizing cryptographic systems with a mediator for securing data in computer networks. We have also studied principles of cryptographic network modeling based on the analysis of a graph of a computer network. The execution results of the developed model provided us the ability to define the CET-operations sets applicable for creating a cryptographic network. Finally, we have studied the attributes of simultaneous functioning of both computer and cryptographic networks. The main foundation of our research is a hypothesis postulating the possibility of creating a cryptographic network by simultaneously utilizing regular cryptographic networks and cryptographic networks with mediators, which are created based on CET-operations. We define a cryptographic network as a cryptographic system adapted for data security in computer or telecommunication networks based on encryption, decryption, and re-encryption of data. The results of the conducted simulation experiment and defined CET-operations sets confirm the effectiveness of the described principles of modeling a cryptographic network as an add-on for a computer network. A cryptographic network is less complex in terms of configuration in comparison to sets of cryptographic systems. It also greatly increases the number of options and combinations of network construction. In addition, network addressees can modify cryptograms, thus further increasing the variability of an algorithm used for ensuring network functioning. The dependence of both the model of cryptographic network and CET-operations sets on network structure and architecture creates additional obstacles for hackers. Finally, there are numerous options for solving a model of cryptographic network. This provides an option to apply multiple-key technologies of stream encryption based on the non-symmetrical commutative and non-commutative CET-operations.

Keywords

limited resources cryptography, cryptography, post-quantum cryptography, cryptographic networks, CET-encryption, CET-operations, two-operand CET-operations

1. Introduction

Cryptographic security of confidential data in computer systems and networks is an extremely important matter. Achieving improvements in this field requires effective and complex methods of data security during its storage [1, 2], transmission [3, 4], and processing [5]. The size of data resources for storage, transmission and processing is the defining attribute for choosing methods of cryptographic data security. The size of data resources affects the efficiency of computer networks, as well as the system of cryptographic security. It is worth noting, however, that an increase in the efficiency of computer network may result in a reduction of resources available for allocation for

*CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine
*Corresponding author.
†These authors contributed equally.
rvn_2008@ukr.net (V. Rudnytskyi); v.babenko@chdtu.edu.ua (V. Babenko); ladanatali256@gmail.com (N. Lada); tatiana_ami@ukr.net (T. Stabetska); d.a.pidlasyi.asp22@chdtu.edu.ua (D. Pidlasyi); liubomyr.t.parkhuts@lpnu.ua (L. Parkhuts)
0000-0003-3473-7433 (V. Rudnytskyi); 0000-0003-2039-2841 (V. Babenko); 0000-0002-7682-2970 (N. Lada); 0000-0001-9192-5313 (T. Stabetska); 0000-0002-9916-5256 (D. Pidlasyi); 0000-0003-4759-9383 (L. Parkhuts)

cryptographic data protection. An effective method for mitigating this downside is implementing lightweight cryptography in secured computer networks [6–9]. This necessity to apply the lightweight cryptography in computer networks exists due to the different effectiveness of cryptographic algorithms used for securing the stored, transfered and processed data [10].

Effective functioning of cryptographic system for data security within computer network is ensured primarily by balancing such attributes as cryptographic integrity, complexity and speed of execution, as well as available resources. In addition, the structure, architecture and performance features of the computer network should also be taken into account during projection of the data security systems [11]. One effective solution for optimization of this attribute revolves around the creation of cryptographic systems based on CET-operations (Cryptographic Encoding Theory). These operations are an integral part of CET-encryption [11].

2. Analysis of sources and target setting

The analytical review of the results of research related to CET-operations is available in [12]. The vital role of non-commutative CET-operations among the two-operand CET-operations is an important factor to consider. This is primarily because of the sheer quantity of non-commutative CET-operations (including non-symmetrical) compared to the commutative CET-operations (including non-symmetrical) [11]. Scientists have dedicated numerous researches to study their attributes and applications. For example, paper [13] describes options for creating stream ciphers based on double-cycle non-commutative CET-operations. Monograph [11] generalizes the research results revolving around CET-operations and stream encryption technologies based on these operations. We, however, have dedicated our paper to researching the attributes of cryptographic systems with a mediator, as well as the peculiarities of their creation. The main attribute of such system is the presence of a mediator that re-encrypts a cryptogram before transmitting it to one of the addressees. This re-encryption ensures confidentiality of encryption, decryption, and re-encryption algorithms within the cryptographic system with one or several mediators. Monograph [11] suggests the option for creating cryptographic networks based on cryptographic systems with a mediator similar to computer networks. The authors have analyzed the principles of creating cryptographic networks as cryptographic add-ons for computer networks with identical structure and architecture. In theory, this cryptographic network is capable of ensuring the confidentiality of stored, transmitted, and processed data by keeping encryption, decryption, and re-encryption algorithms confidential. However, the authors of the monograph [11] only assume the possibility of such cryptographic networks, and this assumption is proved neither theoretically, nor practically.

Recent studies in the field of applied cryptography also emphasize the importance of practical implementation aspects when designing secure communication architectures. For instance, the work of Vorobets et al. [14] investigates the integration of post-quantum key encapsulation mechanisms in real-world environments, which could be adapted for mediator-based network structures. Similarly, Sovyn et al. [15] explore methods for optimizing cryptographic components, such as S-boxes, which may improve the efficiency of CET-based encryption. Additionally, research by Opirskyy et al. [16] addresses potential vulnerabilities in information systems at different TCP/IP layers, highlighting threat models relevant for secure mediator-based communication channels.

3. Purpose and objectives of research

The main purpose is the development of principles applicable to modeling of cryptographic network with the defined architecture, as well as the definition of CET-operations sets to ensure the correct functionality of this network.

We have established the following objectives to fulfill the aforementioned purpose:

- To analyze the attributes of cryptographic data security in computer networks.

- To analyze the attributes of utilizing the cryptographic systems with a mediator for securing data in computer networks.
- To create a model of cryptographic network based on the analysis of a graph of a computer network.
- To define the CET-operations sets applicable for creation of a cryptographic network based on the execution results of the created model.
- To analyze the execution attributes of a cryptographic network for the defined CET-operations sets.

4. Materials and methods

The object of our research is the processes of data transformation under conditions of joint usage of the limited resources stream ciphers based on CET-operations.

The main hypothesis serving as the foundation of our research is the possibility of creating a cryptographic network by joint usage of regular cryptographic systems and cryptographic systems with mediators, which are created based on CET-operations. Processes, such as encryption, decryption, and re-encryption of confidential data, are ensured by the network addressees by executing the defined CET-operations sets. Joint application of these processes substantially increases the variability of CET-encryption.

The first step of proving the hypothesis lies in practical confirmation of the possibility to define the CET-operations set applicable to setting up a cryptographic network with defined architecture. Discovering the relationships between CET-operations and defining their sets requires creation of constraint system with multiple options for limiting cryptographic transformations according to the architecture of cryptographic network. We can consider this system of limitations as a model of cryptographic network. To create the model of cryptographic network, we have used methods of discrete mathematics, set theory and linear algebra.

We will use only single- and two-operand CET-operations to present the results of our research. To simplify the presentation of these practical results, we use only 2 Ci-quanta CET-operations. We apply this limitation because of having only one mathematical apparatus used to describe an entire set of CET-operations in the field G_4 [11].

5. Modeling of a cryptographic network based on application of CET-operations

Transmission of confidential data in computer networks proceeds from sender to receiver. If there is no direct link from sender to receiver, the mediator will be responsible for retransmission of a cryptogram.

The exchange of confidential data is ensured for every pair of addressees by utilization of a cryptographic system for data encryption and decryption. However, these systems do not take into account presence or absence of mediators for retransmission of a cryptogram. Implementing separate cryptographic systems for data exchange in the secured computer network increases the complexity of data security system. Overall, the complexity increases proportionally to the number of addressees in computer network. This particular approach, however, does not take into account structure and architecture of a computer network, as well as the attributes of cryptographic systems with a mediator.

We will now analyze creation of data security system in computer network based on CET-operations and cryptographic systems with a mediator. We will refer to this data security system as cryptographic network. The cryptographic network ensures data security in computer network, and thus requires identical network architecture for proper functioning. A structure of a computer network defines the requirements for creating a cryptographic network, while the results of creating said cryptographic network impose limitations on functionality of a computer network.

We will now analyze the possibility of creating data security system in computer network based on CET-operations. Let's assume, that a computer network consists of 5 addressees and is presented by an oriented graph. Graphs of both the computer and cryptographic networks are identical due to the identical architecture of these networks. Creation of a cryptographic network can be analyzed by its representation graph from Figure 1.

Let's assume, that addressees of a cryptographic network can transmit data directly, and through mediators. Ensuring direct exchange of confidential data between different addressees requires implementing different CET-encryption algorithms.

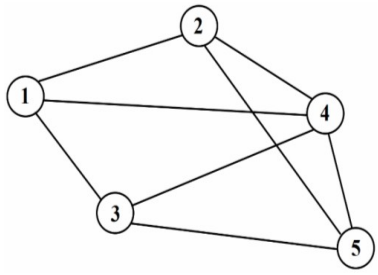

Figure 1: Graph of a cryptographic (computer) network

We impose the following limitations during creation of a cryptographic network:

- non-symmetrical CET-operations are preferable for establishing cryptographic link between addresses.
- identical models of CET-operations are preferable for decreasing complexity of the cryptographic network for direct and inverse cryptographic transformations.
- a minimal number of addressees is required during the establishment of a cryptographic link.

Taking into account these limitations, we will now analyze option 1 in detail.

First, we will describe the limitations of direct cryptographic links between addressees within the cryptographic network. Let's assume, that addressee 1 directly transmits data to addressee 2. The data is encrypted by CET-operation $C_{1,2}(x)$. Addressee 1 then acquires data from addressee 2. The data is encrypted by CET-operation $C_{2,1}(x)$. The cryptographic link between addressees 1 and 2 can be established under the following conditions:

$$\begin{cases} C_{1,2}(x) \neq C_{2,1}(x); \\ C_{2,1}(C_{1,2}(x)) = x, \;\; C_{2,1}(x) = C'_{1,2}(x); \\ C_{1,2}(C_{2,1}(x)) = x, \;\; C_{1,2}(x) = C'_{2,1}(x). \end{cases} \tag{1}$$

Addressee 1 directly transmits data to addressee 3. The data is encrypted by CET-operation $C_{1,3}(x)$. Addressee 1 then acquires data from addressee 3. The data is encrypted by CET-operation $C_{3,1}(x)$. The cryptographic link between addressees 1 and 3 can be established under the following conditions:

$$\begin{cases} C_{1,3}(x) \neq C_{3,1}(x); \\ C_{3,1}(C_{1,3}(x)) = x, \;\; C_{3,1}(x) = C'_{1,3}(x); \\ C_{1,3}(C_{3,1}(x)) = x, \;\; C_{1,3}(x) = C'_{3,1}(x). \end{cases} \tag{2}$$

Addressee 1 directly transmits data to addressee 4. The data is encrypted by CET-operation $C_{1,4}(x)$. Addressee 1 then acquires data from addressee 4. The data is encrypted by CET-operation

$C_{4,1}(x)$. The cryptographic link between addressees 1 and 4 can be established under the following conditions:

$$\begin{cases} C_{1,4}(x) \neq C_{4,1}(x); \\ C_{4,1}(C_{1,4}(x)) = x, \;\; C_{4,1}(x) = C'_{1,4}(x); \\ C_{1,4}(C_{4,1}(x)) = x, \;\; C_{1,4}(x) = C'_{4,1}(x). \end{cases} \tag{3}$$

Addressee 2 directly transmits data to addressee 4. The data is encrypted by CET-operation $C_{2,4}(x)$. Addressee 2 then acquires data from addressee 4. The data is encrypted by CET-operation $C_{4,2}(x)$. The cryptographic link between addressees 2 and 4 can be established under the following conditions:

$$\begin{cases} C_{2,4}(x) \neq C_{4,2}(x); \\ C_{4,2}(C_{2,4}(x)) = x, \;\; C_{4,2}(x) = C'_{2,4}(x); \\ C_{2,4}(C_{4,2}(x)) = x, \;\; C_{2,4}(x) = C'_{4,2}(x). \end{cases} \tag{4}$$

Addressee 2 directly transmits data to addressee 5. The data is encrypted by CET-operation $C_{2,5}(x)$. Addressee 2 then acquires data from addressee 5. The data is encrypted by CET-operation $C_{5,2}(x)$. The cryptographic link between addressees 2 and 5 can be established under the following conditions:

$$\begin{cases} C_{2,5}(x) \neq C_{5,2}(x); \\ C_{5,2}(C_{2,5}(x)) = x, \;\; C_{5,2}(x) = C'_{2,5}(x); \\ C_{2,5}(C_{5,2}(x)) = x, \;\; C_{2,5}(x) = C'_{5,2}(x). \end{cases} \tag{5}$$

The conditions for establishing all direct cryptographic links illustrated in Figure 1 are described similarly to those analyzed above.

Having generalized the limitations related to direct cryptographic links between addressees within the cryptographic network, we can now further proceed with our analysis.

$$\begin{cases} C_{1,2}(x) = C'_{2,1}(x); \quad C_{2,1}(x) = C'_{1,2}(x); \quad C_{1,2}(x) \neq C_{2,1}(x); \\ C_{1,3}(x) = C'_{3,1}(x); \quad C_{3,1}(x) = C'_{1,3}(x); \quad C_{1,3}(x) \neq C_{3,1}(x); \\ C_{1,4}(x) = C'_{4,1}(x); \quad C_{4,1}(x) = C'_{1,4}(x); \quad C_{1,4}(x) \neq C_{4,1}(x); \\ C_{2,4}(x) = C'_{4,2}(x); \quad C_{4,2}(x) = C'_{2,4}(x); \quad C_{2,4}(x) \neq C_{4,2}(x); \\ C_{2,5}(x) = C'_{5,2}(x); \quad C_{5,2}(x) = C'_{2,5}(x); \quad C_{2,5}(x) \neq C_{5,2}(x); \\ C_{3,4}(x) = C'_{4,3}(x); \quad C_{4,3}(x) = C'_{3,4}(x); \quad C_{3,4}(x) \neq C_{4,3}(x); \\ C_{3,5}(x) = C'_{5,3}(x); \quad C_{5,3}(x) = C'_{3,5}(x); \quad C_{3,5}(x) \neq C_{5,3}(x); \\ C_{4,5}(x) = C'_{5,4}(x); \quad C_{5,4}(x) = C'_{4,5}(x); \quad C_{4,5}(x) \neq C_{5,4}(x); \end{cases}$$

We will now describe the limitations of cryptographic links with a mediator between addressees within the cryptographic network.

Addressee 1 can establish a cryptographic link with addressee 5 with assistance of addressee 2 acting as a mediator.

The cryptographic link based on (1) and (5) cannot be established because:

- $C_{5,2}(C_{2,5}(C_{1,2}(x))) = C_{1,2}(x) \neq x$. This expression is valid because $C_{5,2}(C_{2,5}(x)) = x$.

- $C_{5,2}(C_{2,1}(C_{1,2}(x)))= C_{5,2}(x)\neq x$. This expression is valid because $C_{2,1}(C_{1,2}(x))= x$. When a mediator operates with an inverse CET-operation, the data is decrypted before being transmitted to the addressee (or another mediator), thus resulting in a loss of confidentiality.

Dealing with the issue mentioned above is possible by ensuring that addressee operates with different CET-operations for data decryption. Addressee 1 uses the following 3 CET-operations according to models (1)–(4): $C_{1,2}(x)$, $C_{1,3}(x)$ and $C_{1,4}(x)$. Thus, the establishment of confidential communications link through addressee 2 requires utilization of the following models: $C_{1,3}(x)$, $C_{1,4}(x)$.

$$C_{5,2}(C_{2,1}(C_{1,3}(x))) = x;\ C_{5,2}(C_{2,1}(C_{1,4}(x))) = x.$$

$C_{5,2}(x)= const$ and $C_{2,1}(x)= const$ are valid for the described models. Thus, only one operation can be used for modeling a cryptographic system with communications link between addressees 1 and 5 through addressee 2 acting as a mediator. This operation is either $C_{1,3}(x)$, or $C_{1,4}(x)$. The validity of this claim is based on a fact that single-operand CET-operations used for encryption are from one mathematical group of operations to an accuracy of permutation. Thus, we can acquire the following results:

$$\left\langle \begin{matrix} C_{5,2}(C_{2,1}(C_{1,3}(x))) = x \\ C_{5,2}(C_{2,1}(C_{1,4}(x))) = x \end{matrix} \right. \quad (6)$$

where $\langle$ indicates that a transformation is possible by solving at least one equation (model).

Similarly, we will now create models of other relationships through mediators.
Addressee 1 can establish a cryptographic link with addressee 5 in several ways:

- with assistance of addressee 3 acting as a mediator. This can be done under the following conditions:

$$\left\langle \begin{matrix} C_{5,3}(C_{3,1}(C_{1,2}(x))) = x \\ C_{5,3}(C_{3,1}(C_{1,4}(x))) = x \end{matrix} \right. \quad (7)$$

- with assistance of addressee 4 acting as a mediator. This can be done under the following condition:

$$\left\langle \begin{matrix} C_{5,4}(C_{4,1}(C_{1,2}(x))) = x \\ C_{5,4}(C_{4,1}(C_{1,3}(x))) = x \end{matrix} \right. \quad (8)$$

Cryptographic network is capable of ensuring transmission of confidential data from addressee 1 to addressee 4 if at least one condition ((6), (7), or (9)) is fulfilled.

$$\left\langle \begin{matrix} \left\langle \begin{matrix} C_{5,2}(C_{2,1}(C_{1,3}(x))) = x \\ C_{5,2}(C_{2,1}(C_{1,4}(x))) = x \end{matrix} \right. \\ \left\langle \begin{matrix} C_{5,3}(C_{3,1}(C_{1,2}(x))) = x \\ C_{5,3}(C_{3,1}(C_{1,4}(x))) = x \end{matrix} \right. \\ \left\langle \begin{matrix} C_{5,4}(C_{4,1}(C_{1,2}(x))) = x \\ C_{5,4}(C_{4,1}(C_{1,3}(x))) = x \end{matrix} \right. \end{matrix} \right.$$

Simultaneous fulfillment of several conditions ensures transmission of confidential data through several routes and different mediators.

The limitations for other routes used for exchange of confidential data between addressees through mediators are defined similarly.

Combining these limitations provides an opportunity to create a model of cryptographic network described in Figure 1.

$$
\begin{cases}
\left\langle \begin{array}{l} C_{5,2}(C_{2,1}(C_{1,3}(x))) = x \\ C_{5,2}(C_{2,1}(C_{1,4}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{5,3}(C_{3,1}(C_{1,2}(x))) = x \\ C_{5,3}(C_{3,1}(C_{1,4}(x))) = x \end{array} \right. ; \\
\left\langle \begin{array}{l} C_{5,4}(C_{4,1}(C_{1,2}(x))) = x \\ C_{5,4}(C_{4,1}(C_{1,3}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{3,1}(C_{1,2}(C_{2,4}(x))) = x \\ C_{3,1}(C_{1,2}(C_{2,5}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{3,4}(C_{4,2}(C_{2,1}(x))) = x \\ C_{3,4}(C_{4,2}(C_{2,5}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{3,5}(C_{5,2}(C_{2,1}(x))) = x \\ C_{3,5}(C_{5,2}(C_{2,5}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{2,1}(C_{1,3}(C_{3,4}(x))) = x \\ C_{2,1}(C_{1,3}(C_{3,5}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{2,4}(C_{4,3}(C_{3,1}(x))) = x \\ C_{2,4}(C_{4,3}(C_{3,5}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{2,5}(C_{5,3}(C_{3,1}(x))) = x \\ C_{2,5}(C_{5,3}(C_{3,4}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{1,2}(C_{2,5}(C_{5,3}(x))) = x \\ C_{1,2}(C_{2,5}(C_{5,4}(x))) = x \end{array} \right. \\
\left\langle \begin{array}{l} C_{1,3}(C_{3,5}(C_{5,2}(x))) = x \\ C_{1,3}(C_{3,5}(C_{5,4}(x))) = x \end{array} \right. \\
\begin{cases}
C_{1,2}(x) = C_{2,1}^{/}(x); \quad C_{2,1}(x) = C_{1,2}^{/}(x); \quad C_{1,2}(x) \neq C_{2,1}(x); \\
C_{1,3}(x) = C_{3,1}^{/}(x); \quad C_{3,1}(x) = C_{1,3}^{/}(x); \quad C_{1,3}(x) \neq C_{3,1}(x); \\
C_{1,4}(x) = C_{4,1}^{/}(x); \quad C_{4,1}(x) = C_{1,4}^{/}(x); \quad C_{1,4}(x) \neq C_{4,1}(x); \\
C_{2,4}(x) = C_{4,2}^{/}(x); \quad C_{4,2}(x) = C_{2,4}^{/}(x); \quad C_{2,4}(x) \neq C_{4,2}(x); \\
C_{2,5}(x) = C_{5,2}^{/}(x); \quad C_{5,2}(x) = C_{2,5}^{/}(x); \quad C_{2,5}(x) \neq C_{5,2}(x); \\
C_{3,4}(x) = C_{4,3}^{/}(x); \quad C_{4,3}(x) = C_{3,4}^{/}(x); \quad C_{3,4}(x) \neq C_{4,3}(x); \\
C_{3,5}(x) = C_{5,3}^{/}(x); \quad C_{5,3}(x) = C_{3,5}^{/}(x); \quad C_{3,5}(x) \neq C_{5,3}(x); \\
C_{4,5}(x) = C_{5,4}^{/}(x); \quad C_{5,4}(x) = C_{4,5}^{/}(x); \quad C_{4,5}(x) \neq C_{5,4}(x);
\end{cases}
\end{cases}
\tag{9}
$$

We can define a set of single-operand CET-operations for creating a cryptographic network based on single-operand CET-operations by solving a system of equations (9). These equations establish limitations in the defined cryptographic network. Several solutions for the system of equations (9) results in acquisition of several sets of single-operand CET-operations. Single-operand CET-operations from different sets can be combined either into groups of single-operand CET-operations or into multi-operand CET-operations. This allows creating cryptographic networks based on groups of CET-operations or multi-operand CET-operations.

We will use a group of 2Ci-quanta single-operand CET-operations to define a set of single-operand CET-operations to create a cryptographic network described in Figure 1 according to model (9). The group of 2Ci-quanta single-operand CET-operations is described in Table 1 [11]. Non-symmetrical single-operand CET-operations usable during creation of a cryptographic network are highlighted in grey.

Table 1

Group of 2Ci-quanta single-operand CET-operations [11]

2Ci-quanta single-operands			
$C_1(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$C_7(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$C_{13}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{19}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$C_2(x)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$C_8(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$C_{14}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	$C_{20}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$C_3(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$C_9(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	$C_{15}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$C_{21}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$C_4(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{10}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{16}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{22}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$
$C_5(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{11}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{17}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{23}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$
$C_6(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$	$C_{12}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$C_{18}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	$C_{24}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$

Having conducted our simulation experience, we have acquired the following number of options for implementing a cryptographic network (Figure 1) based on 2 Ci-quanta single-operand CET-operations: CET-operations: $\approx 3{,}9 \cdot 10^6$. All of the acquired options apply to solving the equations system (9).

We will now analyze one of these options:

The expression below describes how addressee 1 encrypts data for addressee 2: $C_{1.2}(x)=C_7(x)=C_8^{/}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$. Expression below describes how addressee 1 encrypts data for addressee 3: $C_{1.3}(x)=C_8(x)=C_7^{/}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 1 encrypts data for addressee 4: $C_{1.4}(x)=C_{10}(x)=C_{18}^{/}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$.

Expression below describes how addressee 2 encrypts data for addressee 1: $C_{2.1}(x) = C_8(x) = C_7^{/}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 2 encrypts data for addressee 4: $C_{2.4}(x) = C_7(x) = C_8^{/}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$. Expression below describes how addressee 2 encrypts data for addressee 5: $C_{2.5}(x) = C_{10}(x) = C_{18}^{/}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$.

Expression below describes how addressee 3 encrypts data for addressee 1: $C_{3.1}(x) = C_7(x) = C_8^{/}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$. Expression below describes how addressee 3 encrypts data for addressee 4: $C_{3.4}(x) = C_8(x) = C_7^{/}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 3 encrypts data for addressee 5: $C_{3.5}(x) = C_{13}(x) = C_{11}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$.

Expression below describes how addressee 4 encrypts data for addressee 1: $C_{4.1}(x) = C_{18}(x) = C_{10}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 4 encrypts data for addressee 2: $C_{4.2}(x) = C_8(x) = C_7^{/}(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 4 encrypts data for addressee 3: $C_{4.3}(x) = C_7(x) = C_8^{/}(x) = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$. Expression below describes how addressee 4 encrypts data for addressee 5: $C_{4.5}(x) = C_{11}(x) = C_{13}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$.

Expression below describes how addressee 5 encrypts data for addressee 2: $C_{5.2}(x) = C_{18}(x) = C_{10}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$. Expression below describes how addressee 5 encrypts data for addressee 3: $C_{5.3}(x) = C_{11}(x) = C_{13}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$. Expression below describes how addressee 5 encrypts data for addressee 4: $C_{5.4}(x) = C_{13}(x) = C_{11}^{/}(x) = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$.

Addressee 1 encrypts data for addressee 5 by CET-operation $C_{1.4}(x) = C_{10}(x)$. If transmission occurs through addressee 3, then the following operation is valid: $C_{5.3}(C_{3.1}(C_{1.4}(x))) = x$. If transmission occurs through addressee 4, then CET-operation $C_{1.3}(x) = C_8(x)$ is used for encryption and the following operation is valid: $C_{5.4}(C_{4.1}(C_{1.3}(x))) = x$.

Addressee 2 encrypts data for addressee 3 by CET-operation $C_{2.1}(x) = C_8(x)$. Transmission occurs through addressee 5: $C_{3.5}(C_{5.2}(C_{2.1}(x))) = x$.

Addressee 3 encrypts data for addressee 2 by CET-operation $C_{3.1}(x) = C_7(x)$. Transmission occurs through addressee 5: $C_{2.5}(C_{5.3}(C_{3.1}(x))) = x$.

Addressee 5 encrypts data for addressee 1 by CET-operation $C_{5.3}(x)=C_{11}(x)$. Transmission occurs through addressee 2: $C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$. If transmission occurs through addressee 4, then CET-operation $C_{1.3}(x)=C_{8}(x)$ is used for encryption and the following operation is valid: $C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$. Table 2 shows all the described cryptographic relationships between addressees of cryptographic network (Figure 1). Models used for transformation of data through mediator are highlighted in grey.

Table 2
An option for implementing a cryptographic network

Addressees of crypto-graphic network	Addressee 1	Addressee 2	Addressee 3	Addressee 4	Addressee 5
Addressee 1	———	$C_{1.2}(x)=C_{7}(x)$	$C_{1.3}(x)=C_{8}(x)$	$C_{1.4}(x)=C_{10}(x)$	$C_{5.3}(C_{3.1}(C_{1.4}(x)))=x$ $C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$
Addressee 2	$C_{2.1}(x)=C_{8}(x)$	———	$C_{3.5}(C_{5.2}(C_{2.1}(x)))=x$	$C_{2.4}(x)=C_{7}(x)$	$C_{2.5}(x)=C_{10}(x)$
Addressee 3	$C_{3.1}(x)=C_{7}(x)$	$C_{2.5}(C_{5.3}(C_{3.1}(x)))=x$	———	$C_{3.4}(x)=C_{8}(x)$	$C_{3.5}(x)=C_{13}(x)$
Addressee 4	$C_{4.1}(x)=C_{18}(x)$	$C_{4.2}(x)=C_{8}(x)$	$C_{4.3}(x)=C_{7}(x)$	———	$C_{4.5}(x)=C_{11}(x)$
Addressee 5	$C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$ $C_{1.3}(C_{3.5}(C_{5.2}(x)))=x$	$C_{5.2}(x)=C_{18}(x)$	$C_{5.3}(x)=C_{11}(x)$	$C_{5.4}(x)=C_{13}(x)$	———

Model (9) is applicable for creation of cryptographic networks based on either the models of single-operand CET-operations, or models of multi-operand CET-operations.

We will now analyze creation of a cryptographic network defined by a graph from Figure 1 based on 2Ci-quanta two-operand CET-operations. Doing so requires us to pick 4 options from the set of acquired options for implementing a cryptographic network based on single-operand CET-operations. CET-operations related to these options must operate with identical models for data transmission through mediator.

The 4 randomly selected options are described in tables from Table 3 to Table 6.

Table 3
An option for implementing a cryptographic network

Addressees of crypto-graphic network	Addressee 1	Addressee 2	Addressee 3	Addressee 4	Addressee 5
Addressee 1	———	$C_{1.2}(x)=C_{7}(x)$	$C_{1.3}(x)=C_{8}(x)$	$C_{1.4}(x)=C_{10}(x)$	$C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$
Addressee 2	$C_{2.1}(x)=C_{8}(x)$	———	$C_{3.5}(C_{5.2}(C_{2.1}(x)))=x$	$C_{2.4}(x)=C_{7}(x)$	$C_{2.5}(x)=C_{23}(x)$
Addressee 3	$C_{3.1}(x)=C_{7}(x)$	$C_{2.5}(C_{5.3}(C_{3.1}(x)))=x$	———	$C_{3.4}(x)=C_{24}(x)$	$C_{3.5}(x)=C_{19}(x)$
Addressee 4	$C_{4.1}(x)=C_{18}(x)$	$C_{4.2}(x)=C_{8}(x)$	$C_{4.3}(x)=C_{15}(x)$	———	$C_{4.5}(x)=C_{11}(x)$
Addressee 5	$C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$ $C_{1.3}(C_{3.5}(C_{5.2}(x)))=x$	$C_{5.2}(x)=C_{12}(x)$	$C_{5.3}(x)=C_{22}(x)$	$C_{5.4}(x)=C_{13}(x)$	———

Table 4
An option for implementing a cryptographic network

Addressees of cryptographic network	Addressee 1	Addressee 2	Addressee 3	Addressee 4	Addressee 5
Addressee 1	———	$C_{1.2}(x)=C_{10}(x)$	$C_{1.3}(x)=C_{18}(x)$	$C_{1.4}(x)=C_{7}(x)$	$C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$
Addressee 2	$C_{2.1}(x)=C_{18}(x)$	———	$C_{3.5}(C_{5.2}(C_{2.1}(x)))=x$	$C_{2.4}(x)=C_{22}(x)$	$C_{2.5}(x)=C_{16}(x)$
Addressee 3	$C_{3.1}(x)=C_{10}(x)$	$C_{2.5}(C_{5.3}(C_{3.1}(x)))=x$	———	$C_{3.4}(x)=C_{11}(x)$	$C_{3.5}(x)=C_{23}(x)$
Addressee 4	$C_{4.1}(x)=C_{8}(x)$	$C_{4.2}(x)=C_{19}(x)$	$C_{4.3}(x)=C_{13}(x)$	———	$C_{4.5}(x)=C_{22}(x)$
Addressee 5	$C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$ $C_{1.3}(C_{3.5}(C_{5.2}(x)))=x$	$C_{5.2}(x)=C_{20}(x)$	$C_{5.3}(x)=C_{12}(x)$	$C_{5.4}(x)=C_{19}(x)$	———

Table 5
An option for implementing a cryptographic network

Addressees of cryptographic network	Addressee 1	Addressee 2	Addressee 3	Addressee 4	Addressee 5
Addressee 1	———	$C_{1.2}(x)=C_{11}(x)$	$C_{1.3}(x)=C_{13}(x)$	$C_{1.4}(x)=C_{8}(x)$	$C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$
Addressee 2	$C_{2.1}(x)=C_{13}(x)$	———	$C_{3.5}(C_{5.2}(C_{2.1}(x)))=x$	$C_{2.4}(x)=C_{10}(x)$	$C_{2.5}(x)=C_{7}(x)$
Addressee 3	$C_{3.1}(x)=C_{11}(x)$	$C_{2.5}(C_{5.3}(C_{3.1}(x)))=x$	———	$C_{3.4}(x)=C_{16}(x)$	$C_{3.5}(x)=C_{18}(x)$
Addressee 4	$C_{4.1}(x)=C_{7}(x)$	$C_{4.2}(x)=C_{18}(x)$	$C_{4.3}(x)=C_{20}(x)$	———	$C_{4.5}(x)=C_{12}(x)$
Addressee 5	$C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$ $C_{1.3}(C_{3.5}(C_{5.2}(x)))=x$	$C_{5.2}(x)=C_{8}(x)$	$C_{5.3}(x)=C_{10}(x)$	$C_{5.4}(x)=C_{23}(x)$	———

Table 6
An option for implementing a cryptographic network

Addressees of cryptographic network	Addressee 1	Addressee 2	Addressee 3	Addressee 4	Addressee 5
Addressee 1	———	$C_{1.2}(x)=C_{12}(x)$	$C_{1.3}(x)=C_{23}(x)$	$C_{1.4}(x)=C_{11}(x)$	$C_{5.4}(C_{4.1}(C_{1.3}(x)))=x$
Addressee 2	$C_{2.1}(x)=C_{23}(x)$	———	$C_{3.5}(C_{5.2}(C_{2.1}(x)))=x$	$C_{2.4}(x)=C_{8}(x)$	$C_{2.5}(x)=C_{19}(x)$
Addressee 3	$C_{3.1}(x)=C_{12}(x)$	$C_{2.5}(C_{5.3}(C_{3.1}(x)))=x$	———	$C_{3.4}(x)=C_{10}(x)$	$C_{3.5}(x)=C_{13}(x)$
Addressee 4	$C_{4.1}(x)=C_{13}(x)$	$C_{4.2}(x)=C_{7}(x)$	$C_{4.3}(x)=C_{18}(x)$	———	$C_{4.5}(x)=C_{8}(x)$
Addressee 5	$C_{1.2}(C_{2.5}(C_{5.3}(x)))=x$ $C_{1.3}(C_{3.5}(C_{5.2}(x)))=x$	$C_{5.2}(x)=C_{22}(x)$	$C_{5.3}(x)=C_{11}(x)$	$C_{5.4}(x)=C_{7}(x)$	———

We can sequentially combine the identically named single-operand CET-operations into tuples with 4 operations each to create a set of two-operand CET-operations to implement a cryptographic network. Sequence of single-operand CET-operations in a tuple of two-operand CET-operation must be identical to a sequence of the chosen options for implementing a cryptographic network.

For example:

$$C_{1.2}(x, y) = C_{1.2}((C_{1.2}(x) = C_7(x)), (C_{1.2}(x) = C_{10}(x)), (C_{1.2}(x) = C_{11}(x)), (C_{1.2}(x) = C_{12}(x)))$$

Based on the acquired tuple of single-operand CET-operations, we will now create a two-operand CET-operation [11].

$$C_{1.2}(x, y) = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{bmatrix} (y_1 \cdot \overline{y}_2) \cdot x_1 \oplus x_2 \oplus y_1 \\ (\overline{y}_1 \vee y_2) \cdot x_1 \oplus (\overline{y}_1 \cdot \overline{y}_2) \cdot x_2 \oplus \overline{y}_2 \end{bmatrix}$$

Similarly, we will now create all other two-operand CET-operations used for implementation of a cryptographic network.

$$C_{1.3}(x, y) = \begin{bmatrix} (\overline{y}_1 \cdot \overline{y}_2) \cdot x_1 \oplus x_2 \oplus \overline{y}_1 \cdot \overline{y}_2 \\ (\overline{y}_1 \vee y_2) \cdot x_1 \oplus (y_1 \cdot \overline{y}_2) \cdot x_2 \oplus y_1 \end{bmatrix}$$

$$C_{1.4}(x, y) = \begin{bmatrix} (y_1 \cdot y_2) \cdot x_1 \oplus x_2 \oplus y_1 \\ (\overline{y}_1 \vee \overline{y}_2) \cdot x_1 \oplus (y_1 \equiv y_2) \cdot x_2 \oplus y_2 \end{bmatrix}$$

$$C_{2.1}(x, y) = \begin{bmatrix} (y_1 \vee y_2) \cdot x_1 \oplus x_2 \oplus \overline{y}_1 \cdot \overline{y}_2 \\ (y_1 \vee \overline{y}_2) \cdot x_1 \oplus (y_1 \cdot \overline{y}_2) \cdot x_2 \oplus y_1 \end{bmatrix}$$

$$C_{2.4}(x, y) = \begin{bmatrix} (y_1 \cdot \overline{y}_2) \cdot x_1 \oplus (y_1 \vee \overline{y}_2) \cdot x_2 \oplus \overline{y}_2 \\ x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus \overline{y}_1 \cdot \overline{y}_2 \end{bmatrix}$$

$$C_{2.5}(x, y) = \begin{bmatrix} (y_1 \equiv y_2) \cdot x_1 \oplus (y_1 \vee y_2) \cdot x_2 \oplus y_2 \\ x_1 \oplus y_2 \cdot x_2 \oplus (\overline{y}_1 \vee y_2) \end{bmatrix}$$

$$C_{3.1}(x, y) = \begin{bmatrix} (y_1 \cdot \overline{y}_2) \cdot x_1 \oplus x_2 \oplus y_1 \\ (y_1 \vee \overline{y}_2) \cdot x_1 \oplus (y_1 \vee y_2) \cdot x_2 \oplus (y_1 \vee \overline{y}_2) \end{bmatrix}$$

$$C_{3.4}(x, y) = \begin{bmatrix} \overline{y}_1 \cdot x_1 \oplus x_2 \oplus (\overline{y}_1 \vee \overline{y}_2) \\ (y_1 \vee \overline{y}_2) \cdot x_1 \oplus (y_1 \vee y_2) \cdot x_2 \oplus (\overline{y}_1 \cdot y_2) \end{bmatrix}$$

$$C_{3.5}(x, y) = \begin{bmatrix} x_1 \oplus (y_1 \vee y_2) \cdot x_2 \oplus \overline{y}_1 \cdot y_2 \\ (\overline{y}_1 \cdot \overline{y}_2) \cdot x_1 \oplus (y_1 \equiv y_2) \cdot x_2 \oplus (\overline{y}_1 \vee y_2) \end{bmatrix}$$

$$C_{4.1}(x, y) = \begin{bmatrix} (y_1 \equiv y_2) \cdot x_1 \oplus x_2 \oplus \overline{y}_1 \cdot y_2 \\ (\overline{y}_1 \vee \overline{y}_2) \cdot x_1 \oplus (\overline{y}_1 \cdot \overline{y}_2) \cdot x_2 \oplus y_1 \end{bmatrix}$$

$$C_{4.2}(x,y)=\begin{bmatrix}(y_1\oplus y_2)\cdot x_1\oplus(y_1\vee\overline{y}_2)\cdot x_2\oplus\overline{y}_1\\ x_1\oplus(\overline{y}_1\cdot y_2)\cdot x_2\oplus y_2\end{bmatrix}$$

$$C_{4.3}(x,y)=\begin{bmatrix}(y_1\oplus y_2)\cdot x_1\oplus x_2\oplus y_1\cdot y_2\\ (y_1\vee\overline{y}_2)\cdot x_1\oplus\overline{y}_1\cdot x_2\oplus(\overline{y}_1\vee\overline{y}_2)\end{bmatrix}$$

$$C_{4.5}(x,y)=\begin{bmatrix}\overline{y}_1\cdot x_1\oplus(y_1\vee\overline{y}_2)\cdot x_2\oplus 1\\ (y_1\vee y_2)\cdot x_1\oplus(\overline{y}_1\vee\overline{y}_2)\cdot x_2\oplus\overline{y}_2\end{bmatrix}$$

$$C_{5.2}(x,y)=\begin{bmatrix}y_2\cdot x_1\oplus(\overline{y}_1\vee\overline{y}_2)\cdot x_2\oplus 1\\ x_1\oplus(y_1\equiv y_2)\cdot x_2\oplus\overline{y}_1\end{bmatrix}$$

$$C_{5.3}(x,y)=\begin{bmatrix}(y_1\equiv y_2)\cdot x_1\oplus(y_1\vee y_2)\cdot x_2\oplus(\overline{y}_1\vee y_2)\\ (\overline{y}_1\vee\overline{y}_2)\cdot x_1\oplus x_2\oplus y_2\end{bmatrix}$$

$$C_{5.3}(x,y)=\begin{bmatrix}(\overline{y}_1\vee\overline{y}_2)\cdot x_1\oplus(y_1\vee\overline{y}_2)\cdot x_2\oplus(\overline{y}_1\vee y_2)\\ (y_1\vee y_2)\cdot x_1\oplus\overline{y}_1\cdot x_2\oplus 1\end{bmatrix}$$

The acquired set of two-operand CET-operations is applicable for transmission of confidential data through mediator within cryptographic network.

Addressee 1 encrypts data for addressee 5 by CET-operation $C_{1,3}(x,y)$. If transmission occurs through addressee 4, then the following operation is valid: $C_{3.5}\left(C_{5.2}\left(C_{2.1}(x,y),y\right),y\right)=x$.

Addressee 2 encrypts data for addressee 3 by CET-operation $C_{2,1}(x,y)$. If transmission occurs through addressee 5, then the following operation is valid: $C_{3.5}\left(C_{5.2}\left(C_{2.1}(x,y),y\right),y\right)=x$.

Addressee 3 encrypts data for addressee 2 by CET-operation. If transmission occurs through addressee 5, then the following operation is valid: $C_{2.5}\left(C_{5.3}\left(C_{3.1}(x,y),y\right),y\right)=x$.

Addressee 5 encrypts data for addressee 1 by CET-operation $C_{5,3}(x,y)$. If transmission occurs through addressee 2, then the following operation is valid: $C_{1.2}\left(C_{2.5}\left(C_{5.3}(x,y),y\right),y\right)=x$.

If transmission occurs through addressee 4, then CET-operation $C_{1,3}(x,y)$ is used for encryption and the following operation is valid: $C_{5.4}\left(C_{4.1}\left(C_{1.3}(x,y),y\right),y\right)=x$.

The correctness of these models is easily validated if the value of the second operand is fixed (y). We can thus conclude that a cryptographic network created based on two-operand CET-operations can function properly when addressees operate with identical pseudorandom (key) sequences.

6. Results analysis

Data security in computer networks based on implementing cryptographic data security systems greatly increases the complexity of the generic data security system. It occurs because this approach does not take into account the structure and architecture of computer or telecommunication network requiring protection. Adapting data security system to structure and architecture of a network is possible based on cryptographic systems with a mediator [11].

We define a cryptographic network as a cryptographic system adapted for data security in computer or telecommunication networks based on encryption, decryption, and re-encryption of data. We also define CET-encryption as a theoretical foundation for creating cryptographic networks [11]. Addressees can operate with different CET-encryption algorithms and use them jointly to create closed communications links. This reduces the complexity of implementing a cryptographic network. Reduction of complexity is explained by the fact that the number of

algorithms used by each addressee (graph node) is proportional to the number of connected communications links (edges), and not the number of system addressees.

CET-encryption is a branch of lightweight post quantum cryptography [13]. Thus, we can consider cryptographic networks as a type of lightweight post quantum data security systems.

Theoretical possibility of creating a cryptographic network [11] can only be proven by a practical attempt to create the said network.

Our simulation experience conducted based on the created network model has, however, proven the correctness of theoretical recommendations and hypotheses [11]. We have used a group of 2Ci-quanta CET-operations (operations in field G_4) during our experiment. As a result, we have acquired $\approx 3{,}9 \cdot 10^6$ number of options for implementing a cryptographic network based on single-operand CET-operations. We have acquired this result based on just 24 operations from the group. Thus, we have decided not to use a group of 3Ci-quanta CET-operations (40320 operations in the field G_8), or a group of 4Ci-quanta CET-operations (16! operations in the field G_{16}) during our experiment.

The quantity of acquired sets applicable to implementing a cryptographic network allows us to combine single-operand CET-operations into multi-operand operations. Multi-operand CET-operations are highly recommended for use during creation of both cryptographic systems and networks due to the great increase in the cryptographic integrity and variance of cryptographic transformations. In cryptographic networks these operations are also applicable to implementing different stream encryption technologies based on CET-encryption [11]. According to defined limitations, non-symmetrical CET-operations, including commutative, non-commutative and mutually inverse, can be used during creation of a cryptographic network [11–13]. Overall, the acquired results apply to creating lightweight cryptographic networks for securing data in mobile or stationary computer and telecommunication networks [17–20].

We would like to note, that the attributes of any multi-operand CET-operation are defined by the attributes of a set of single-operand CET-operations used to create it. During creation of a cryptographic network, however, the sets of single-operand CET-operations required for ensuring proper operation are defined pseudorandomly based on sorting. This is because a cryptographic network is impossible to synthesize with predefined attributes of cryptographic transformation. We believe this to be the primary downside of this research. Nevertheless, it is possible to address this by implementing additional limitations into the model of a cryptographic network. These limitations are related to the attributes of single-operand operations and attributes of the result of the recurring cryptographic transformation.

Conclusions

We consider moving from cryptographic systems to cryptographic networks for securing data in computer and telecommunication networks the next stage in the development of cryptography. Utilization of generic cryptographic systems and cryptographic systems with mediators based on CET-operations lays the foundation for creating cryptographic networks while taking into account their structure and architecture.

We define technology applicable to the development of a cryptographic network with defined architecture as a development sequence of a model of limitations for functioning of a cryptographic network, as well as a sequence of defining sets of CET-operations.

A cryptographic network is less complex in terms of configuration in comparison to sets of cryptographic systems. It also greatly increases the number of options and combinations of network construction. In addition, network addressees can modify cryptograms, thus further increasing the variability of an algorithm used for ensuring network functioning. The dependence of both the model of cryptographic network and CET-operations sets on network structure and architecture creates additional obstacles for hackers.

Finally, there are numerous options for solving a model of cryptographic network. This provides an option to apply multiple-key technologies of stream encryption based on the non-symmetrical commutative and non-commutative CET-operations.

We suggest further research to improve cryptographic network modeling to identify ways of defining sets of CET-operations with predefined attributes.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] T. Eldem, Global Cyberspace Security and Critical Information Infrastructure Protection, Global Encyclopedia of Public Administration, Public Policy, and Governance. Springer, Cham, 2021. doi:10.1007/978-3-319-31816-5_3987-1

[2] P. Keshattiwar, P. Lokulwar, P. Saraf, Empowering Data Defender's Comprehensive Security Measures for Robust Information Protection in Robust-Cloud Environments, in: 2024 Int. Conf. on Innovations and Challenges in Emerging Technologies (ICICET), 2024, 1–6 doi:10.1109/ICICET59348.2024.10616293

[3] P. Atri, Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit, Int. J. Comput. Eng. 5(4) (2024) 44–55. doi:10.47941/ijce.1920

[4] J. M. Borky, T. H. Bradley, Protecting Information with Cybersecurity. In: Effective Model-based Systems Engineering, Springer, Cham, 2019. doi:10.1007/978-3-319-95669-5_10

[5] B. Nadji, Data Security, Integrity, and Protection. In: Data, Security, and Trust in Smart Cities. Signals and Communication Technology, Springer, Cham, 2024. doi:10.1007/978-3-031-61117-9_4

[6] S. Pandey, B. Bhushan, Recent Lightweight Cryptography (LWC) based Security Advances for Resource-Constrained IoT Networks, Wireless Netw. 30 (2024) 2987–3026. doi:10.1007/s11276-024-03714-4

[7] T.J.E. Dandin, D. Krishnaveni, K. Chandrasekhar, Light Weight Cryptography and Its Application in Resource Constrained Environment Using Reversible Logic, in: 2nd Int. Conf. on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Lecture Notes in Networks and Systems, 237, 2022. doi:10.1007/978-981-16-6407-6_43

[8] N. Yasmin, R. Gupta, Modified Lightweight Cryptography Scheme and Its Applications in IoT Environment. Int. J. Inf. Tecnol. 15 (2023) 4403–4414. doi:10.1007/s41870-023-01486-2

[9] A. Zakaria, A. Azni, F. Ridzuan, N. Zakaria, H. Maslina, Daud Systematic Literature Review: Trend Analysis on the Design of Lightweight Block Cipher, IEEE J. King Saud University – Comput. Inf. Sci. 35(5) (2023) 101550. doi:10.1016/j.jksuci.2023.04.003

[10] V. Thakor, A. Razzaque, M. Khandaker, Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities, IEEE Access, 9 (2021) 28177328193. doi:10.1109/ACCESS.2021.3052867

[11] V. Rudnytskyi, N. Lada, G. Kushuk, D. Pidlasyi, Architecture of CET-Operations and Stream Encryption Technologies: Monograph. Cherkasy, 2024. https://dndivsovt.com/index.php/monograph/issue/view/22/22

[12] N. Lada, et al., Development of CET-Encryption Theory: A Comprehensive Review, J. Xidian University, 18(8) (2024) 898-025. doi:10.37896/jxu18.8/079

[13] V. Rudnytskyi, et al., Usage of Non-Commutative Two-Operand CET-Operations in Limited Resources Stream Cipher, J. Xidian University, 18(5) (2024) 1105–1120. doi:10.5281/Zenodo.11253625

[14] P. Vorobets, et al., Implementing Post-Quantum KEMs: Practical Challenges and Solutions, in: Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024), 3826, 2024, 212–219.
[15] Y. Sovyn, et al., Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction, in: Cybersecurity Providing in Information and Telecommunication Systems, 3421, 2023, 12–24.
[16] I. Opirskyy, et al., Evaluation of the Possibility of Realizing the Crime of the Information System at Different Stages of TCP/IP, in: IEEE 4th Int. Conf. Adv. Inf. Commun. Technol. (AICT), 2021, 261–265. doi:10.1109/AICT52120.2021.9628936
[17] A. Ilyenko, et al., Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 226-233.
[18] R. Chernenko, et al., Encryption Method for Systems with Limited Computing Resources, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 142-148.
[19] M. Iavich, et al., Classical and Post-Quantum Encryption for GDPR, in: Classic, Quantum, and Post-Quantum Cryptography, vol. 3829 (2024) 70–78.
[20] A. Horpenyuk, I. Opirskyy, P. Vorobets, Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms, in: Classic, Quantum, and Post-Quantum Cryptography, 3504, 2023, pp. 39–49.