Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2022, № 3 (107) https://doi.org/10.33108/visnyk_tntu2022.03
ISSN 2522-4433. Web: visnyk.tntu.edu.ua

UDC 004.75

EVALUATION OF THE REVERSE TRANSFORMATION METHODS COMPLEXITY OF THE RESIDUAL NUMBER SYSTEM FOR SECURE DATA STORAGE

Serhii Kulyna

West Ukrainian National University, Ternopil, Ukraine

Summary. *The methods of conversion from the residual number system to the decimal number system based on the classical Chinese remainder theorem (CRT) and its improvements CRT I, CRT II are considered in this paper. Analytical dependences of the time complexity of the specified methods are analyzed and constructed. As the result of carried out investigation, it is established that CRT II is characterized by greater efficiency compared to the other methods mentioned above. Examples of the implementation of direct and reverse conversion of RNS based on the application of CRT, CRT I, CRT II are given.*

Key words: *Residual number system, Chinese remainder theorem, distributed data storage, reverse transformation methods, secure data storage systems.*

https://doi.org/10.33108/visnyk_tntu2022.03.021 *Received 15.06.2022*

Statement of the problem. In the modern world tendencies, the increase of the efficiency of the method of storing information on distributed and cloud services is one of the most important problems in the field of IT technologies. When using them, we usually face the problem of increasing trust in these services, ensuring confidentiality and data integrity in the process of transmission, processing and storage.

Analysis of available investigation results. The investigations aimed at the development and use of homomorphic data encryption methods for their use in cloud services are actively carried out in the world [1, 2]. Despite existing researches, there are still many unsolved problems that reduce trust in modern cloud and remote data storage services [3–5]. One of the ways to increase the reliability and security of data storage systems is the use of residual number system (RNS) [6, 7].

The objective of the paper is to carry out investigation of the time complexity of methods of reverse conversion of RNS, which will allow to increase the efficiency of distributed data storage systems based on RNS to construct analytical dependences of the time complexity of the specified methods, to justify the choice of effective reverse transformation method.

Statement of the task. In the previous papers, the use of RNS for secure distributed data storage was investigated [8]. The essence of this method is to divide data into fragments and store individual fragments on different cloud or distributed services. Thus, data protection is achieved due to the fact that in order to restore them, it is necessary to access all fragments stored in the cloud storage of various providers or on physically distributed media.

In order to divide the data into fragments, the method of direct transformation of RNS is used, that is, the distribution of the information package or file content into the system of mutually simple modules, and the fragments themselves are distributed on the appropriate cloud or remote storage (Fig. 1).

Corresponding author: Serhii Kulyna; e-mail: sersks@gmail.com

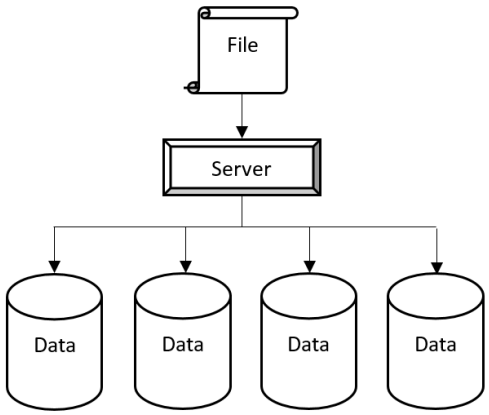

Figure 1. Distribution of the information package into fragments

In RNS, data recovery is usually performed by reverse transformation [9, 10]. Comparative analysis of the methods of classical Chinese remainder theorem (CRT) and its modifications: the new Chinese remainder theorem I (CRT I) and the new Chinese remainder theorem II (CRT II) [11] is carried out in this paper.

Theoretical presentation. Distribution of information into fragments is carried out according to the formula [12]:

$$x_i = X mod\ p_i, \tag{1}$$

where X is information presented in the positional numbering system; p_i are mutually simple modules.

Received information packages are stored on remote or distributed storage. In order to restore data, the classic reverse transformation of RNS is used [11]:

$$X = (\sum_{i=1}^{n} x_i b_i)\ mod\ M, \tag{2}$$

where $M = \prod_1^n p_i$, and b_i are base numbers of RCS, which are calculated according to the following formula:

$$b_i = \frac{M}{p_i} \cdot t_i \equiv 1 mod\ p_i, \tag{3}$$

where t_i is a set of coefficients that ensure orthogonality of transformations and satisfy condition $0 < t_i < p_i$.

Another reverse transformation method considered in this paper is the application of the new Chinese Remainder Theorem I (CRT I). In this case, the initial information is restored according to the following formula [11]:

$$\begin{gathered} X = [\mathrm{x}_0 + t_0 p_0 (\mathrm{x}_1 - \mathrm{x}_0) + t_1 p_0 p_1 (\mathrm{x}_2 - \mathrm{x}_1) + \cdots \\ \cdots + t_{n-1} p_0 p_1 * \cdots * p_{n-1} (\mathrm{x}_n - \mathrm{x}_{n-1})]\ mod\ M, \end{gathered} \tag{4}$$

where t_i is a set of coefficients that ensure orthogonality of transformations and satisfy the following condition:

$$t_i = (\prod_1^j p_i)^{-1} mod\ (\prod_{j+1}^n p_i). \tag{5}$$

The new Chinese Remainder Theorem 2 (CRT II) is also considered while analyzing

the existing restoration methods. The comparison of the complexity of information restoration is carried out for the system of 4 modules. According to the given task, data restoration takes place according to the formula [11]:

$$X = N_2 + [k_2(N_1 - N_2)] mod\ M, \quad (6)$$

where N_1 and N_2 are calculated according to the following formulas:

$$N_1 = x_1 + [k_0(x_0 - x_1)] mod\ p_0 p_1; \quad (7)$$

$$N_2 = x_3 + [k_1(x_2 - x_3)] mod\ p_3. \quad (8)$$

The above-mentioned formulas (6–8) use a set of coefficients k_i that must satisfy the following equalities:

$$k_0 p_1 \equiv 1 \bmod p_0; \quad (9)$$

$$k_1 p_3 \equiv 1 \bmod p_2; \quad (10)$$

$$k_3 p_2 p_3 \equiv 1 \bmod (p_0 p_1). \quad (11)$$

As the result of the calculation of each of the above-mentioned data recovery methods, we get the initial value *X*.

Example. Let's consider examples of the implementation of each of the above-mentioned reverse transformation methods. Let's take the system of modules with minimal values p_i=[3, 5, 7, 11], *n*=4.

The total range of the system of modules is $M = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$, and the working one is $R = 3 \cdot 5 \cdot 7 = 315$.

For an example, let us consider the distribution and recovery of the information message X=80 presented in the decimal number system.

The indicated number in the system of remainders according to formula (1) in the corresponding modules will have the form X_i=[2, 0, 3, 3].

Using each of these methods, we will restore the initial value X.

Method 1. In order to restore the number according to CRT, we calculate the base values according to formula 3:

$$b=[385, 231, 330, 210].$$

When substituting the corresponding values b_i and x_i we get (formula 2):

$$X_j=(x_0 b_0+x_1 b_1+x_2 b_2+x_3 b_3) \bmod M=(2 \cdot 385 + 0 \cdot 231 + 3 \cdot 330 + +3 \cdot 210) \bmod 1155 = 2390 \bmod 1155 = 80.$$

Method 2. In order to restore the numbers according to CRT I (formula 4), we find a set of coefficients t_i according to formula 5:

$$t_0=(p_0)^{-1} mod\ (p_1 p_2 p_3) = (3)^{-1} mod\ (385) = 257;$$

$$t_1=(p_0 p_1)^{-1} mod\ (p_2 p_3) = (15)^{-1} mod\ (77) = 36;$$

$$t_2=(p_0 p_1 p_2)^{-1} mod\ p_3 = (105)^{-1} mod\ (11) = 2.$$

By substituting the remainders x_i and coefficients t_i into formula 3, we get the desired value X:

$$X_j = [x_0 + t_0p_0(x_1 - x_0) + t_1p_0p_1(x_2 - x_1) + t_2p_0p_1p_2(x_3 - x_2)]\ mod\ M = [2 + 257 \cdot 3 \cdot \cdot (0 - 2) + 36 \cdot 3 \cdot 5 \cdot (3 - 0) + 2 \cdot 3 \cdot 5 \cdot 7 \cdot (3 - 3)] mod\ 1155 = [2 + (-1542) + 1620 + 0] mod\ 1155 = 80.$$

Method 3. When using the new Chinese remainder theorem 2 (CRT II), we calculate the values according to equalities (9–11):

$$k_0p_1 \equiv 1 \bmod p_0 = 5k_1 \equiv 1 \bmod 3, k_0 = 2;$$

$$k_1p_3 \equiv 1 \bmod p_2 = 11k_1 \equiv 1 \bmod 7, k_1 = 2;$$

$$k_2p_2p_3 \equiv 1 \bmod (p_0p_1) = 77k_3 \equiv 1 \bmod 15, k_2 = 8.$$

After the calculation of coefficients k_i, the next step is to find the values N_1 and N_2:

$$N_1 = x_1 + ([k_0(x_0 - x_1)] mod\ p_0)p_1 = 0 + [2(2 - 0)] mod\ 3 \cdot 5 = 5;$$

$$N_2 = x_3 + [k_1(x_2 - x_3)] mod\ p_3 = 3 + [2 \cdot (3 - 3)] mod\ 11 = 3.$$

According to the results of calculations based on formula (6), we get the restored value X:

$$X = N_2 + [k_2(N_1 - N_2)] mod\ M = 3 + ([8 \cdot (5 - 3)] mod\ 15) \cdot 77 = 80.$$

It should be noted that each of the above-mentioned methods has its own sequence of operations. Some variables such as base numbers b_i, coefficients k_i and t_i for multiple reverse conversion do not need to be calculated each time and can be calculated in advance and saved for later use. This makes it possible to reduce the number of steps and, accordingly, increase the speed of the system as a whole. Some of the proposed methods have significant advantages when implemented in distributed systems [13].

Results of the investigation. In order to conduct investigations of the time complexity of CRT, it is necessary to define a set of basic operations, which include: addition, remainder search, product of k-bit numbers, division [14].

The dependence of the time complexity of basic operations on the bit rate of the input data is presented in Table 1.

Table 1

Time complexity of basic CRT operations

No	Basic operation	Time complexity
1	$x_i = X(mod\ p_i)$	$Q_1(k+1)^2 \approx Q_1(k^2 + 2 \cdot k)$
2	$M = \prod_1^n p_i$	$Q_2(n \cdot k^2)$
3	$b_i = \frac{M}{p_i} \cdot t_i \equiv 1 mod\ p_i$	$Q_3(2 \cdot k^2)$
4	$X = (\sum_{i=1}^n x_i b_i)\ mod\ M$	$Q_4(n \cdot (k^2 + (k+1)^2)) \approx \approx Q_4(2 \cdot n \cdot k^2 + 2 \cdot n \cdot k + n)$

where n is the number of modules, and k is the bit rate of the input data.

While performing calculations, it is also worth considering that some operations, which are an order of magnitude simpler, can be neglected, since they do not affect the overall complexity (for example, formulas 1 and 4 in Table 1).

According to the formulas presented in Table 1, the total complexity of CRT is calculated according to the formula:

$$Q_{crt}(n\cdot((k+1)^2+(n\cdot k^2)+(2\cdot k^2))+(2\cdot n\cdot k^2))=Q_{crt}((n^2\cdot k^2)+(5\cdot n\cdot k^2))\approx \approx Q_{crt}(n^2\cdot k^2) \quad (12)$$

The time complexity of the basic operations of CRT I is given in Table 2.

Table 2

Time complexity of basic CRT I operations

No	Basic operation	Time complexity
1	$X_j = [x_0 + t_0 p_0 (x_1 - x_0) + t_1 \cdot \cdot\ p_0 p_1 (x_2 x_1) \cdots t_{n-1} p_0 p_1 \cdot \cdot \cdots \cdot p_{n-1} \cdot (x_n - x_{n-1})]\ mod\ M$	$Q_5((n\cdot k)^2+(k+1)^2)=Q_5((n+1)\cdot k^2+2\cdot k+1)$
2	$t_{n-1}=(p_1\cdot p_2\cdot p_3\cdot ...p_{n-1})^{-1}\bmod p_n$	$Q_6(35\cdot k^2)$

According to the formulas presented in Table 2, the total complexity of CRT I is:

$$Q_{crt\_I}((n+1)\cdot k^2+2\cdot k+1)+35\cdot k^2)=Q_{crt\_I}((n+1)\cdot k^2+37\cdot k+1)\approx \approx Q_{crt\_I}((n+1)\cdot k^2+37\cdot k) \quad (13)$$

Let's determine the time complexity of basic CRT II operations (Table 3).

Table 3

Time complexity of basic CRT II operations

No	Basic operation	Time complexity
1	$N_1=x_2+[k_1\cdot(x_1-x_2)]\bmod(p_1\cdot p_2)$ $N_2=x_4+[k_2\cdot(x_3-x_4)]\bmod p_4$	$Q_7((k+1)^2+k^2+2\cdot k^2)\approx Q_7(4\cdot k^2)$
2	$X=N_2+[k_3\cdot(N_1-N_2)]\bmod M$	$Q_8((k+1)^2+k^2+2\cdot k^2)\approx Q_8(4\cdot k^2)$
3	$k_1\cdot p_2\equiv 1\bmod p_1$ $k_2\cdot p_4\equiv 1\bmod p_3$ $k_3\cdot p_3\cdot p_4\equiv 1\bmod(p_1\cdot p_1)$	$Q_9(k^2)$

According to the formulas presented in Table 3, the total complexity of CRT II for 4 modules is estimated as:

$$Q_{crt\_II}(9\cdot k^2). \quad (14)$$

Based on the above mentioned calculations, in order to compare the efficiency of using different variations of CRT, it is necessary to plot the dependence of time complexity, taking into account the bit rate and the number of modules.

In order to assess the complexity of the reverse conversion methods, comparison is carried out for RNS from four modules of different bit sizes and, taking into account this condition, we obtained the following values of estimates for each of the methods:

$$Q_{crt}(4^2 \cdot k^2) = Q_{crt}(16 \cdot k^2);$$

$$Q_{crt\_I}(2 \cdot 4 \cdot k^2) = Q_{crt\_I}(8 \cdot k^2);$$

$$Q_{crt\_II}(5 \cdot k^2).$$

The dependence of the time complexity of each above mentioned methods on the bit rate of the input data at $n = 4$ is given in Table 4.

Table 4

The dependence of the time complexity of each on the data bit rate

No	k	Qcrt	Qcrt_I	Qcrt_II
1	16	4096	2048	1280
2	32	16384	8192	5120
3	64	65536	32768	20480
4	128	262144	131072	81920
5	256	1048576	524288	327680
6	512	4194304	2097152	1310720
7	1024	16777216	8388608	5242880

The dependence of the time complexity of the reverse transformation methods is graphically presented in Figure 2.

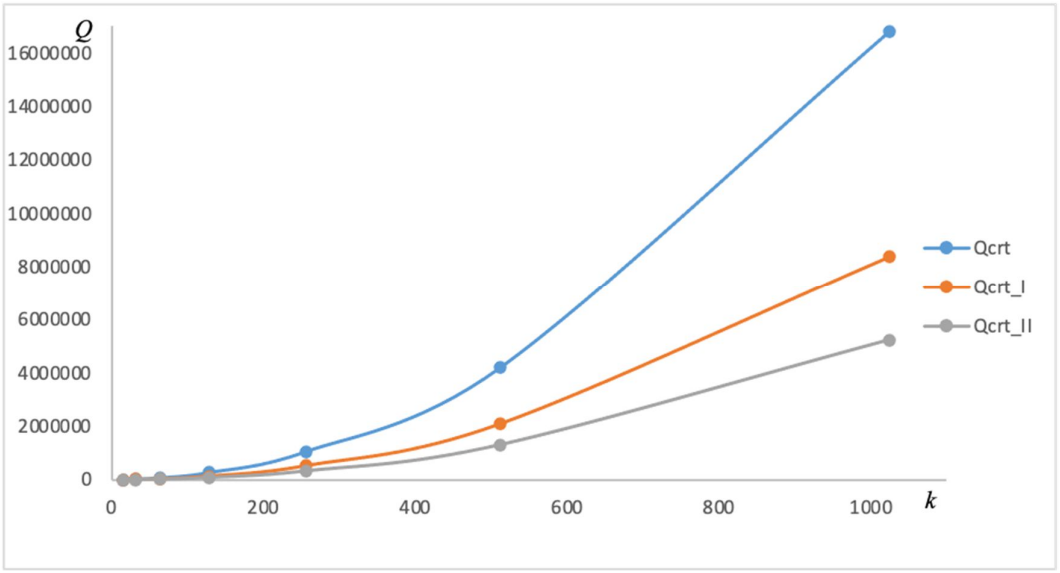

Figure 2. Dependence of the time complexity of CRT, CRT I and CRT II on bit rate k

As the result of the analytical calculations, it should be noted that with small bit size of the modules, each of the methods is characterized by almost the same time complexity, and with the increase in modules bit size, the complexity of calculating the reverse transformation increases significantly. Therefore, the use of CRT I and CRT II according to research results is much more effective for application in secure data storage systems.

Conclusions. In this paper the investigation of time complexity of methods of inverse transformation of RNS for use in the systems of distributed data storage of increased security and reliability is carried out. On the basis of time complexity investigations, the choice of effective reverse transformation method, namely the classical theorem on residues I (CRT I) and II (CRT II), which are characterized by lower time complexity with the increase in the number of modules bits, is justified. Based on Table 4, at the maximum considered bit rate, the complexity of calculations while using CRT I is 2 times lower than while using CRT, and the use of CRT II gives complexity 1.6 times lower compared to CRT I.

Examples of the implementation of the considered methods for the 4-modular residual number system are given, each of the methods has its own sequence of operations. And some variables, such as base numbers b_i, coefficients k_i and t_i are calculated once for multiple reverse conversions, which makes it possible to reduce the number of steps and, accordingly, increase the speed of data conversion and thus increase the efficiency of the system as a whole.

References

1. Mather T., Kumaraswamy S., and Latif S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media, Inc., 2009.
2. LI, Baiyu; Micciancio, D. On the security of homomorphic encryption on approximate numbers. Proc. of 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT 2021–2021, Part I, pp. 648-677, June 2021. DOI: https://doi.org/10.1007/978-3-030-77870-5_23
3. Li, W., Yang, Y., Yuan, D. A Novel Cost-Effective Dynamic Data Replication Strategy for Reliability in Cloud Data Centres. In Proceedings of the 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney, NSW, Australia, 12–14 December 2011, pp. 496–502. DOI: https://doi.org/10.1109/DASC.2011.95
4. Huang, C., Simitci, H., Xu, Y., Ogus, A., Calder, B., Gopalan, P., Li, J., Yekhanin, S. Erasure coding in windows azure storage. In Proceedings of the 2012 USENIX Annual Technical Conference (USENIXATC 12), Boston, MA, USA, 13–15 June 2012, pp. 15–26.
5. Kar A., Sur K., Godara S., Basak S., Mukherjee D., Sukla A. S., ... & Choudhury, R. Secuirity in cloud storage: An enhanced technique of data storage in cloud using RNS. In 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2016. October. P. 1–4. DOI: https://doi.org/10.1109/UEMCON.2016.7777905
6. Yatskiv V., Tsavolyk T., Yatskiv N. The Correcting Codes Formation Method Based on the Residue Number System. Conference Proceedings of 14 th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017) 21-25 February 2017 Polyana-Svalyava. Ukraine. 2017. P. 237–240. DOI: https://doi.org/10.1109/CADSM.2017.7916124
7. Schoinianakis D. Residue arithmetic systems in cryptography: a survey on modern security applications. Journal of Cryptographic Engineering. 10 (3). 2020. P. 249–267. DOI: https://doi.org/10.1007/s13389-020-00231-w
8. Yatskiv, V., Kulyna, S., Yatskiv N., Kulyna H. Protected Distributed Data Storage Based on Residue Number System and Cloud Services. Proc. of 10th International Conference on Advanced Computer Information Technologies. ACIT 2020–2020. P. 796–799. DOI: https://doi.org/10.1109/ACIT49673.2020.9208849
9. Omondi A.R., Premkumar A.B. Residue Number Systems: Theory and Implementation; World Scientific: Singapore, 2007. DOI: https://doi.org/10.1142/p523
10. Mohan, A. Residue Number Systems. Theory and Applications; Springer International Publishing: Cham, Switzerland, 2016.
11. Yuke Wang, Residue-to-Binary Converters Based On New Chinese Remainder Theorems. IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing. Vol. 47. No. 3. March 2000. P. 197–205. DOI: https://doi.org/10.1109/82.826745
12. Akushskyj Y. Ja., Judyckyj D.Y. Mashynnaja aryfmetyka v ostatochnykh klassakh. M.: Sov. radyo. 1968. p. 460.
13. Papachristodoulou, L. Fournaris, A.P. Papagiannopoulos, K. Batina, L. Practical Evaluation of Protected Residue Number System Scalar Multiplication. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018. 2019. P. 259–282. DOI: https://doi.org/10.46586/tches.v2019.i1.259-282

14. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A Method for Decimal Number Recovery from its Residues Based on the Addition of the Product Modules. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2019): Proceedings of the 10th International Conference. 2019. V. 1. P. 13–17. DOI: https://doi.org/10.1109/IDAACS.2019.8924395

UDC 004.75

ОЦІНЮВАННЯ СКЛАДНОСТІ МЕТОДІВ ЗВОРОТНОГО ПЕРЕТВОРЕННЯ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ДЛЯ ЗАХИЩЕНОГО ЗБЕРІГАННЯ ДАНИХ

Сергій Кулина

Західноукраїнський університет, Тернопіль, Україна

Резюме. *В тенденціях сучасного світу однією із актуальних проблем у сфері інформаційних технологій є підвищення ефективності методів зберігання інформації в розподілених та хмарних сервісах. При використанні їх зазвичай виникає проблема підвищення довіри до даних сервісів, забезпечення конфіденційності та цілісності даних у процесі передавання, опрацювання та зберігання. У світі активно проводяться дослідження, направлені на розроблення та використання методів гомоморфного шифрування з метою забезпечення довіри до хмарних сервісів. Не зважаючи на існуючі дослідження, залишається чимало невирішених завдань, які знижують довіру до сучасних хмарних та віддалених сервісів зберігання даних. Одним із напрямків підвищення надійності та захищеності систем зберігання даних є використання системи залишкових класів (СЗК). У попередніх роботах досліджено використання СЗК для захищеного розподіленого зберігання даних. Суть підходу полягає в поділі даних на фрагменти та зберігання окремих фрагментів на різних хмарних чи розподілених сервісах. Таким чином, захист даних досягається завдяки тому, що для їх відновлення необхідно отримати доступ до всіх фрагментів, які зберігаються у хмарних сховищах різних провайдерів або на фізично розподілених носіях. Для поділу даних на фрагменти використовується метод прямого перетворення СЗК, тобто ділення інформаційного пакета чи вмісту файла на систему взаємно простих модулів, а самі фрагменти розподіляються на відповідних хмарних чи віддалених сховищах. У СЗК відновлення даних зазвичай виконується шляхом зворотного перетворення з використанням китайської теореми про залишки. У роботі проведено порівняльний аналіз методів на основі класичної китайської теореми про залишки (КТЗ) та її модифікацій: нової китайської теореми про залишки I (КТЗ I) та нової китайської теореми про залишки II (КТЗ II). Слід відзначити, що кожен з вище згаданих методів має свою послідовність виконання операцій. Деякі змінні, такі, як базисні числа b_i, коефіцієнти k_i та t_i для багаторазового зворотного перетворення не потрібно обчислювати кожного разу і можна обчислити заздалегідь та зберегти для подальшого використання. Це дозволяє зменшити кількість кроків та відповідно збільшити швидкодію роботи системи в цілому. Деякі із запропонованих методів мають значні переваги при реалізації у розподілених системах. На основі проведених обчислень для порівняння ефективності використання різних варіантів КТЗ побудовано графік залежності часових складностей із врахуванням розрядності та кількості модулів. Для оцінювання складності методів зворотного перетворення в роботі проведено порівняння для СЗК із чотирьох модулів різної розрядності. В результаті проведених аналітичних розрахунків слід відмітити, що при невеликій розрядності модулів кожен із методів характеризується практично однаковою часовою складністю, а при збільшенні розрядності модулів суттєво зростає складність обчислення зворотного перетворення. Тому використання КТЗ I і КТЗ II згідно з результатами досліджень є значно ефективнішим для використання в системах захищеного зберігання даних. Проведено дослідження часової складності методів зворотного перетворення СЗК для використання в системах розподіленого зберігання даних підвищеної захищеності та надійності. На основі проведених досліджень часової складності обґрунтовано вибір ефективного методу зворотного перетворення, а саме класичної теореми про залишки I (КТЗ I) та II (КТЗ II), які характеризуються меншою часовою складністю при зростанні розрядності модулів. При максимальній розглянутій розрядності складність обчислень при використанні КТЗ I у 2 рази нижча, ніж при КТЗ, а використання КТЗ II забезпечує складність, нижчу в 1,6 раза в порівнянні із КТЗ I.*

Ключові слова: *система залишкових класів, китайська теорема про залишки, розподілене зберігання даних, методи зворотного перетворення, захищені системи зберігання даних.*

https://doi.org/10.33108/visnyk_tntu2022.03.021 *Отримано 15.06.2022*