ABSTRACT AND REFERENCES

MATHEMATICS AND CYBERNETICS – APPLIED ASPECTS

DOI: 10.15587/1729-4061.2018.151090

SUBSTANTIATION OF CORRECTNESS AND ADVANTAGES OF LENSTRA FACTORIZATION METHOD ON EDWARDS CURVES (p. 6-14)

Lyudmyla Kovalchuk
Institute of Foreign Intelligence Service of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-2874-7950

Oleksij Bespalov
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-7126-6752

Nataliia Kuchynska
Institute of Foreign Intelligence Service of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-6457-7525

Polina Seliukh
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-0027-6037

Artem Zhylin
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-4959-612X

Vasyl Tsurkan
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-1352-042X

The factorization problem, which is the basis for many classical asymmetric cryptosystems (RSA, Rabin, and others) and a cryptographically strong generator of pseudo-random sequences (PBS), has been investigated in this paper. The methods that served as prototypes for the Lenstra method were described, the method for factorization of numbers, which is analogous to the Lenstra method on Edwards curves, has been proposed. To substantiate the correctness of the method, an appropriate mathematical apparatus was developed. In addition, an analog of the Lenstra method on Edwards curves was constructed with the use of the presented apparatus; the appropriate algorithm for the factorization of numbers was designed. The correctness of the method and correctness of the algorithm operation were substantiated mathematically; the top analytical estimates of its performance speed, as well as the lower estimates of success probability, have been strictly proved. The advantages of the developed method in comparison with the classical Lenstra method, which applies elliptic curves in the Weierstrass form, were presented and strictly substantiated. A comparative analysis of the new and the classical algorithms was performed.

Results of the research provided a strict proof that the new algorithm on full Edwards curves, in comparison with the classic one, has some advantages in terms of performance speed, by about 1.5 times. The presented experimental results show that the performance speed increases even larger (by up to 30 per cent) in case the twisted and quadratic curves are used instead of full Edwards curves. It was shown that the assessment of probability of success of the new method increases due to the emergence of new conditions that lead to success of the algorithm that are not satisfied for the classical Lenstra algorithm on Weierstrass curves.

The obtained results make it possible to decrease the time required for solving the problem on factorization by approximately 1.5 times, and thus, enable the faster breaking of cryptosystems whose stability is based on this problem.

Keywords: RSA cryptosystem, factorization problem, factorization methods, Lenstra method, Edwards curves.

References

1. Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W. et. al. (2010). Factorization of a 768-Bit RSA Modulus. Lecture Notes in Computer Science, 333–350. doi: https://doi.org/10.1007/978-3-642-14623-7_18
2. Bouvier, C., Imbert, L. (2018). Faster cofactorization with ECM using mixed representations. IACR Cryptology ePrint Archive, 669.
3. Lenstra, A. K. (2017). General Purpose Integer Factoring. Topics in Computational Number Theory Inspired by Peter L. Montgomery, 116–160. doi: https://doi.org/10.1017/9781316271575.006
4. Lenstra, A. K., Lenstra, H. W. Jr. (1987). Algorithms in number theory. Technical Report 87-008. Chicago: University of Chicago.
5. Lenstra, H. W. Jr. (1986). Elliptic curves and number-theoretic algorithms. Report 86-19. Amsterdam: Mathematisch Instituut, Universiteit van Amsterda.
6. Lenstra, H. W. (1987). Factoring Integers with Elliptic Curves. The Annals of Mathematics, 126 (3), 649. doi: https://doi.org/10.2307/1971363
7. Koblitz, N. (1994). A Course in Number Theory and Cryptography. Springer, 235. doi: https://doi.org/10.1007/978-1-4419-8592-7
8. Solov'ev, Yu. P., Sadovnichiy, V. A., Shavgurlidze, E. T., Belokurov, V. V. (2003). Ellipticheskie krivye i sovremennye algoritmy teorii chisel. Moscow: Izhevsk, 192.
9. Bernstein, D. J., Birkner, P., Lange, T., Peters, C. (2012). ECM using Edwards curves. Mathematics of Computation, 82 (282), 1139–1179. doi: https://doi.org/10.1090/s0025-5718-2012-02633-0
10. Hisil, H., Wong, K. K.-H., Carter, G., Dawson, E. (2008). Twisted Edwards Curves Revisited. Lecture Notes in Computer Science, 326–343. doi: https://doi.org/10.1007/978-3-540-89255-7_20
11. Gélin, A., Kleinjung, T., Lenstra, A. K. (2016). Parametrizations for Families of ECM-friendly curves. IACR Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2016/1092.pdf

12. Edwards, H. M. (2007). A normal form for elliptic curves. Bulletin of the American Mathematical Society, 44 (03), 393–423. doi: https://doi.org/10.1090/s0273-0979-07-01153-6
13. Bernstein, D. J., Lange, T. (2007). Faster Addition and Doubling on Elliptic Curves. Lecture Notes in Computer Science, 29–50. doi: https://doi.org/10.1007/978-3-540-76900-2_3
14. Pollard, J. M. (1974). Theorems on factorization and primality testing. Mathematical Proceedings of the Cambridge Philosophical Society, 76 (03), 521. doi: https://doi.org/10.1017/s0305004100049252
15. Bessalov, A. V. (2017). Ellipticheskie krivye v forme Edvardsa i kriptografiya. Kyiv, 272.
16. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C. (2008). Twisted Edwards Curves. Lecture Notes in Computer Science, 389–405. doi: https://doi.org/10.1007/978-3-540-68164-9_26
17. Bessalov, A. V., Kovalchuk, L. V. (2015). Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field. Cybernetics and Systems Analysis, 51 (2), 165–172. doi: https://doi.org/10.1007/s10559-015-9709-x
18. Bessalov, A. V., Dihtenko, A. A. (2013). Cryptographically resistant Edwards curves over prime fields. Applied Radio Electronics, 12 (2), 285–291.
19. Bespalov, O. Yu., Kuchynska, N. V. (2017). Kryva Edvardsa nad kiltsem lyshkiv yak dekartiv dobutok kryvykh Edvardsa nad skinchenymy poliamy. Prikladnaya radioelektronika, 16 (3-4), 170–175.

DOI: 10.15587/1729-4061.2018.150870

APPLICATION OF THE BASIC MODULE'S FOUNDATION FOR FACTORIZATION OF BIG NUMBERS BY THE FERMAT METHOD (p. 14-23)

Stepan Vynnychuk
Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-0605-1576

Yevhen Maksymenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-4947-2247

Vadym Romanenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-8668-177X

The Fermat method is considered to be the best for factorization of numbers $N=p\times q$ in case of close p and q. Computational complexity of the basic algorithm of the method is determined by the number of check values of X when solving equation $Y^2=X^2N$, as well as by complexity of the arithmetic operations. To reduce it, it is proposed to consider admissible those of test values X, for which $(X^2–N)$modbb is quadratic residue modulo bb, called basic. Application of basic foundation of module bb makes it possible to decrease the number of check X by the number of times, close to $Z=bb/bb^*$, where bb^* is the number of elements of set T of the roots of equation $(Ymodb)^2modb=((Xmodb)^2–Nmodb)modb$, and Z is the acceleration coefficient.

It was determined that magnitude Z(N, bb) is affected by the value of residues Nmodp (at p=2, Nmod8 residues are used). The statement of the problem of finding bb with a maximum Z(N, bb) at restrictions for the amount of memory of the computer, where exponents of prime numbers – multipliers bb – are determined, and the method of its solution were proposed.

To decrease the number of arithmetic operations with big numbers, it was proposed that instead of them to perform the operations with the values of differences between the nearest values of elements T. Then arithmetic operations of multiplication and addition with big numbers are performed only in rare cases. And if we derive the square root of $X^2–N$ only in cases, where the values of $(X^2–N)$modb will be quadratic residues for many foundations of module b, other than bb, the computational complexity of this operation can be neglected.

It was established that the proposed modified algorithm of the Fermat method for numbers 2^{1024} ensures a decrease in computational complexity compared to the basic algorithm on average by 10^7 times.

Keywords: factorization, Fermat method, computational complexity, basic foundation, thinning, quadratic residues.

References

1. Brown, D. (2005). Breaking RSA may be as difficult as factoring. Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2005/380.pdf
2. Aggarwal, D., Maurer, U. (2009). Breaking RSA generically is equivalent to factoring. Advances in Cryptology – EUROCRYPT 2009. Available at: https://eprint.iacr.org/2008/260.pdf
3. Pomerance, C., Lenstra, H. W., Tijdeman, R. (1982). Analysis and comparison of some integer factoring algorithms. Computational methods in number theory, 1, 89–139.
4. Vasilenko, O. N. (2003). Teoretiko-chislovye algoritmy v kriptografii. Moscow, 328.
5. Ishmuhametov, Sh. T. (2011). Metody faktorizacii natural'nyh chisel. Kazan', 213.
6. Korneyko, A. V., Zhilin, A. V. (2011). Analiz izvestnyh vychislitel'nyh metodov faktorizacii mnogorazryadnyh chisel. Modeliuvannia ta i formatsiyni tekhnolohiyi, 61, 3–13.
7. Howey, E. (2014). Primality Testing and Factorization Methods. Semantic Scholar. Available at: https://www.semanticscholar.org/paper/Primality-Testing-and-Factorization-Methods-Howey/7fd44eb2df7b39716e984d548c28f51d9dc6bbbb
8. Wu, M.-E., Tso, R., Sun, H.-M. (2014). On the improvement of Fermat factorization using a continued fraction technique. Future Generation Computer Systems, 30, 162–168. doi: https://doi.org/10.1016/j.future.2013.06.008
9. Knuth, D. (1997). Art of Computer Programming, Vol. 2. Seminumerical Algorithms. Massachusetts, 762.
10. Bressoud, D. (1989). Factorization and Primality Testing. Springer-Verlag, 237. doi: https://doi.org/10.1007/978-1-4612-4544-5

11. Burton, D. (2012). Elementary Number Theory. TMG, 436.
12. Somsuk, K., Tientanopajai, K. (2017). An Improvement of Fermat's Factorization by Considering the Last m Digits of Modulus to Decrease Computation Time. International Journal of Network Security, 19 (1), 99–111. doi: http://doi.org/10.6633/IJNS.201701.19(1).11
13. Somsuk, K., Kasemvilas, S. (2013). MFFV2 and MNQSV2: Improved Factorization Algorithms. 2013 International Conference on Information Science and Applications (ICISA). doi: https://doi.org/10.1109/icisa.2013.6579415
14. Somsuk, K., Kasemvilas, S. (2014). MFFV3: An Improved Integer Factorization Algorithm to Increase Computation Speed. Advanced Materials Research, 931-932, 1432–1436. doi: https://doi.org/10.4028/www.scientific.net/amr.931-932.1432
15. Usman, M., Bajwa, Z., Afza, M. (2015). New Factoring Algorithm: Prime Factoring Algorithm. International Journal of Engineering and Management Research, 5 (1), 75–77. Available at: https://pdfs.semanticscholar.org///10d5/4bf2a4b8f46a99effa195077024d82212683.pdf
16. Somsuk, K., Kasemvilas, S. (2014). Possible Prime Modified Fermat Factorization: New Improved Integer Factorization to Decrease Computation Time for Breaking RSA. Advances in Intelligent Systems and Computing, 325–334. doi: https://doi.org/10.1007/978-3-319-06538-0_32
17. Somsuk, K. (2014). A new modified integer factorization algorithm using integer modulo 20's technique. International Computer Science and Engineering Conference (ICSEC'14), 312–316. Available at: https://www.semanticscholar.org/paper/A-new-modified-integer-factorization-algorithm-20's-Somsuk/d70a527c0a4a7c671c814aad6de140dcbabe4445
18. Wu, M.-E., Tso, R., Sun, H.-M. (2012). On the Improvement of Fermat Factorization. Lecture Notes in Computer Science, 380–391. doi: https://doi.org/10.1007/978-3-642-34601-9_29
19. Vinnichuk, S. D., Maksimenko, E. V. (2016). Mnogokratnoe prorezhivanie dlya uskoreniya metoda faktorizacii Ferma pri neravnomernyh shagah dlya neizvestnoy. Visnyk NTUU "KPI". Informatyka, upravlinnia ta obchysliuvalna, 64, 13–24.
20. Maksymenko, Ye. (2016). Selection of effective basic basis of module with multiple thinning trial value in the factorization fermat's method with irregular pitch. Informatyka ta matematychni metody v modeliuvanni, 6 (3), 270–279.
21. Vynnychuk, S., Maksymenko, Y. (2016). Formation of non-uniformity increment for the basic module base in the problem of fermat's factorization method. Information Technology and Security, 4 (2), 244–254.

DOI: 10.15587/1729-4061.2018.150903

PRACTICAL IMPLEMENTATION OF THE NIEDERREITER MODIFIED CRYPTOCODE SYSTEM ON TRUNCATED ELLIPTIC CODES (p. 24-31)

Serhii Yevseiev
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-1647-6444

Oleksii Tsyhanenko
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-5784-8438

Serhii Ivanchenko
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-1850-9596

Volodymyr Aleksiyev
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-6767-7524

Dmytro Verheles
State Research Institute of Special Communication and Information Protection, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-4417-4398

Sergey Volkov
Odessa State Academy of Technical Regulation and Quality, Odessa, Ukraine
ORCID: http://orcid.org/0000-0002-6559-5290

Roman Korolev
Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-7948-5914

Hryhorii Kots
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-4588-8739

Oleksandr Milov
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-6135-2120

Olexander Shmatko
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0002-2426-900X

On the basis of the practical implementation of the classic Niederreiter scheme for non-binary codes, a pattern has been identified for practical implementation –fixing the admissible position vectors of the plaintext transformation based on equilibrium coding. The obtained set of position vectors of the error vector with a fixed set of masking matrices (the recipient's private key) allows us to obtain the algorithm for decoding the classical Niederreiter crypto-code scheme on non-binary codes. For this, a modification of the crypto-code system (CCS) is necessary. It is proposed to use the additional parameter of key data – the initialization vector (the set of invalid position vectors of the error vector). To counter the Sidelnikov attacks, it is proposed to use modified (shortened) algebraic-geometric (elliptic) codes (MEC). For this, it is necessary to use the second additional initialization vector (the set of positions for shortening the error vector). Based on the modification of the classical Niederreiter scheme on non-binary codes, applied algorithms for generating and decrypting a cryptogram in the Niederreiter

modified crypto-code system based on modified (shortened) elliptic codes and software are proposed. To confirm the profitability of the proposed crypto-code system, the results of the comparative evaluation of energy consumption for the implementation of the classical Niederreiter scheme on elliptic codes and the implementation of the proposed system on modified elliptic codes are presented. The results confirm the possibility of practical implementation of the Niederreiter crypto-code system based on the proposed algorithms. At the same time, the required level of cryptographic strength of the crypto-code system, protection of the cryptosystem against the Sidelnikov attacks and an increase in the rate of cryptographic transformations by 3-5 times compared with the classical Niederreiter scheme are guaranteed.

Keywords: Niederreiter modified crypto-code system, modified shortened elliptic codes, equilibrium coding.

References

1. Grishchuk, R. V., Danik, Yu. G.; Danik, Yu. G. (Ed.) (2016). Osnovy kiberbezopasnosti. Zhitomir: ZHNAEU, 636.
2. Kiberprostranstvo i informacionnyy terrorizm. Available at: http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/
3. Security requirements for cryptographic modules. Available at: https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
4. Ivanchenko, I. S., Khoroshko, V. O., Khokhlachova, Yu. Ye., Chyrkov, D. V. (2013). Zabezpechennia informatsiynoi bezpeky derzhavy. Kyiv: PVP "Zadruha", 170.
5. Kazakova, N. F., Panfilov, V. I., Skachek, L. M., Skopa, O. O., Khoroshk, V. O. (2013). Bezpeka bankivskoi diyalnosti. Kyiv: PVP "Zadruha", 282.
6. Leonenko, G. P., Yudin, A. Yu. (2013). Problemy obespecheniya informacionnoy bezopasnosti sistem kriticheski vazhnoy informacionnoy infrastruktury Ukrainy. Information Technology and Security, 1, 44–48.
7. Evseev, S., Korol', O., Koc, G. (2015). Analysis of the legal framework for the information security management system of the NSMEP. Eastern-European Journal of Enterprise Technologies, 5 (3 (77)), 48–59. doi: https://doi.org/10.15587/1729-4061.2015.51468
8. Yevseiev, S., Tsyhanenko, O. (2018). Development of asymmetrical crypto-coded construction of niderraiter on modified codes. Systemy obrobky informatsiyi, 2 (153), 127–135. doi: https://doi.org/10.30748/soi.2018.153.16
9. Kazakova, N., Pleshko, E., Aivazova, K. (2013). International regulation of regulatory of documents as well standardization in area audit of information security. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 15, 172–181.
10. Kuchuk, G., Kharchenko, V., Kovalenko, A., Ruchkov, E. (2016). Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems. 2016 IEEE East-West Design & Test Symposium (EWDTS). doi: https://doi.org/10.1109/ewdts.2016.7807655
11. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mozhaev, M., Lohvynenko, M. (2017). Multiservice network security metric. 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). doi: https://doi.org/10.1109/aiact.2017.8020083
12. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NIST. doi: https://doi.org/10.6028/nist.ir.8105
13. Dinh, H., Moore, C., Russell, A. (2011). McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks. CRYPTO'11 Proceedings of the 31st annual conference on Advances in cryptology. Santa Barbara, 761–779. Available at: https://dl.acm.org/citation.cfm?id=2033093
14. Achieving 128-bit Security Against Quantum Attacks in OpenVPN. Available at: https://internetscriptieprijs.nl/wp-content/uploads/2017/04/1-Simon-de-Vries-UT.pdf
15. Rossi, M., Hamburg, M., Hutter, M., Marson, M. E. (2017). A Side-Channel Assisted Cryptanalytic Attack Against QcBits. Lecture Notes in Computer Science, 3–23. doi: https://doi.org/10.1007/978-3-319-66787-4_1
16. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D. (2014). Enhanced public key security for the McEliece cryptosystem. Available at: https://arxiv.org/pdf/1108.2462.pdf
17. Cho, J. Y., Griesser, H., Rafique, D. (2017). A McEliece-Based Key Exchange Protocol for Optical Communication Systems. Lecture Notes in Electrical Engineering, 109–123. doi: https://doi.org/10.1007/978-3-319-59265-7_8
18. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18–26. doi: https://doi.org/10.15587/1729-4061.2016.75250
19. Evseev, S. P., Korol, O. H. (2018). Teoretyko-metodolohichni zasady pobudovy hibrydnykh krypto-kodovykh konstruktsiy na zbytkovykh kodakh. Informacionnaya ekonomika: etapy razvitiya, metody upravleniya, modeli. Kharkiv, VSHEM – HNEU im. S. Kuzneca, 233–280.
20. Sidel'nikov, V. M. (2002). Kriptografiya i teoriya kodirovaniya. Materialy konferencii "Moskovskiy universitet i razvitie kriptografii v Rossii". Moscow.
21. Dudykevych, V. B., Kuznetsov, O. O., Tomashevskyi, B. P. (2010). Krypto-kodovyi zakhyst informatsiyi z nedviykovym rivnovahovym koduvanniam. Suchasnyi zakhyst informatsiyi, 2, 14–23.
22. Dudykevych, V. B., Kuznietsov, O. O., Tomashevskyi, B. P. (2010). Metod nedviikovoho rivnovahovoho koduvannia. Suchasnyi zakhyst informatsiyi, 3, 57–68.
23. Zhang, G., Cai, S. (2017). Secure error-correcting (SEC) schemes for network coding through McEliece cryptosystem. Cluster Computing. doi: https://doi.org/10.1007/s10586-017-1294-5
24. Morozov, K., Roy, P. S., Sakurai, K. (2017). On unconditionally binding code-based commitment schemes. Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication – IMCOM '17. doi: https://doi.org/10.1145/3022227.3022327
25. Zhang, G., Cai, S. (2017). Universal secure error-correcting (SEC) schemes for network coding via McEliece crypto-

system based on QC-LDPC codes. Cluster Computing. doi: https://doi.org/10.1007/s10586-017-1354-x
26. Moufek, H., Guenda, K. (2017). A New variant of the McEliece cryptosystem based on the Smith form of convolutional codes. Cryptologia, 42 (3), 227–239. doi: https://doi.org/10.1080/01611194.2017.1362061
27. Biswas, B., Sendrier, N. (2008). McEliece Cryptosystem Implementation: Theory and Practice. Lecture Notes in Computer Science, 47–62. doi: https://doi.org/10.1007/978-3-540-88403-3_4
28. Yevseiev, S., Rzayev, Kh., Tsyhanenko, A. (2016). Analysis of the software implementation of the direct and inverse transform in non-binary equilibrium coding method. Ukrainian Scientific Journal of Information Security, 22 (2), 196–203.
29. Niederreiter, H. (1986). Knapsack-Type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory, 15 (2), 19–34.
30. Rukhin, A., Sota, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S. et. al. (2000). A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication. 2000. doi: https://doi.org/10.6028/nist.sp.800-22

DOI: 10.15587/1729-4061.2018.150848

SYNTHESIS OF THE STRUCTURE OF FUNCTIONAL SYSTEMS OF CONVERSION CLASS WITH A PORTIONAL SUPPLY OF INITIAL PRODUCTS (p. 32-40)

Igor Lutsenko
Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine
ORCID: http://orcid.org/0000-0002-1959-4684

Iryna Oksanych
Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine
ORCID: http://orcid.org/0000-0002-4570-711X

Daria Prykhodko
Kharkiv National Automobile and Highway University, Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0003-3925-4828

Svetlana Koval
Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine
ORCID: http://orcid.org/0000-0002-5178-1332

Olena Feoktystova
National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine
ORCID: http://orcid.org/0000-0001-8490-3108

Iryna Kolos
National University of Food Technologies, Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-7134-1441

The main efforts related to enterprise creation and development are aimed at improving efficiency of resource usage in the enterprise activities. Such problem can be successfully solved only if maximum efficiency is achieved at each stage of the conversion process. In turn, solution of this problem at each separate stage relates to creation of a substantiated structure of an object of functional conversion of source products into end products during the system operation. Such an object capable of functioning with maximum efficiency of resource usage was defined by default as a "functional system".

By the example of a technological process of liquid heating, the problem of synthesizing a functional system of a conversion class with a portioned supply of products of directional effect was solved. In the course of synthesis, the task of ensuring possibility of interaction of the system objects during formation of the end product with required consumer qualities was solved at the first stage.

Architecture of a module for identifying system operations and determining limit values of the effective control range was developed at the second stage of synthesis.

A module linking the level of demand for the end products of the system with optimal control of its productivity was created at the third stage.

Application of the proposed approach has enabled creation of a functional structure with a maximum number of degrees of control freedom. In turn, this solution has made it possible to form an optimal control trajectory depending on consumer demand for end products.

The proposed solution enables use of the synthesized architecture for functional systems of a conversion class with a portioned supply of source products.

Keywords: system synthesis, object structure, cybernetic model, functioning efficiency, operation model.

References

1. Drucker, P. F. (2009). Management: Tasks, Responsibilities, Practices. Harper Collins, 864.
2. Gavrilov, D. A. (2002). Upravlenie proizvodstvom na baze standarta MRP II. Sankt-Peterburg: Piter, 320.
3. Peters, T. J., Waterman, R. H. (1982). In search of excellence (lessons from America's best-run companies). Harper & Row, 400.
4. Barskiy, L. A., Kozin, V. Z. (1978). Sistemniy analiz v obogashchenii poleznyh iskopaemyh. Moscow: Nedra, 486.
5. Aleksandrovskiy, N. M. (1969). Elementy teorii optimal'nyh sistem avtomaticheskogo upravleniya. Moscow: Energiya, 128.
6. Shreyder, Yu. A., Sharov, A. A. (1982). Sistemy i modeli. Moscow: Radio i svyaz', 152.
7. Novikov, D. A. (2016). Kibernetika: Navigator. Istoriya kibernetiki, sovremennoe sostoyanie, perspektivy razvitiya. Moscow: LENAND, 160.
8. Viner, N. (1983). Kibernetika ili upravlenie i svyaz' v zhivotnom i mashine. Moscow: Nauka, 344.
9. Anohin, P. K. (1998). Kibernetika funkcional'nyh sistem. Moscow: Medicina, 400.
10. Ackoff, R., Emery, F. (2005). On Purposeful Systems: An Interdisciplinary Analysis of Individual and Social Behavior as a System of Purposeful Events. New York: Aldine Transaction, 303.
11. Gershenson, C., Csermely, P., Érdi, P., Knyazeva, H., Laszlo, A. (2013). The Past, Present and Future of Cybernetics and

Systems Research. Systems connecting matter, life, culture and technology, 1 (3), 4–13.
12. Kukhar, V., Artiukh, V., Butyrin, A., Prysiazhnyi, A. (2017). Stress-Strain State and Plasticity Reserve Depletion on the Lateral Surface of Workpiece at Various Contact Conditions During Upsetting. Advances in Intelligent Systems and Computing, 201–211. doi: https://doi.org/10.1007/978-3-319-70987-1_22
13. Kukhar, V., Artiukh, V., Prysiazhnyi, A., Pustovgar, A. (2018). Experimental Research and Method for Calculation of 'Upsetting-with-Buckling' Load at the Impression-Free (Dieless) Preforming of Workpiece. E3S Web of Conferences, 33, 02031. doi: https://doi.org/10.1051/e3sconf/20183302031
14. Dragobetskii, V., Zagirnyak, M., Naumova, O., Shlyk, S., Shapoval, A. (2018). Method of Determination of Technological Durabilityof Plastically Deformed Sheet Parts of Vehicles. International Journal of Engineering & Technology, 7 (4.3), 92–99. doi: https://doi.org/10.14419/ijet.v7i4.3.19558
15. Moreau, C., Villares, A., Capron, I., Cathala, B. (2016). Tuning supramolecular interactions of cellulose nanocrystals to design innovative functional materials. Industrial Crops and Products, 93, 96–107. doi: https://doi.org/10.1016/j.indcrop.2016.02.028
16. Lebedev, A. (2017). The Synthesis of Variable Structure System for the Control of Quadrotor Spatial Motion. Applied Mechanics and Materials, 865, 486–491. doi: https://doi.org/10.4028/www.scientific.net/amm.865.486
17. Asanov, A. Z., Dem'yanov, D. N. (2017). Analytical synthesis of a functional observer of the state of a bilinear dynamic system. Avtometriya, 4, 26–34. doi: https://doi.org/10.15372/aut20170403
18. Shimanskiy, R. V., Poleshchuk, A. G., Korol'kov, V. P., Cherkashin, V. V. (2017). Alignment of the writing beam with the diffraction structure rotation axis in synthesis of diffractive optical elements in a polar coordinate system. Avtometriya, 2, 30–38. doi: https://doi.org/10.15372/aut20170203
19. Skoblo, T., Klochko, O., Belkin, E., Sidashenko, A. (2017). Effective Technological Process of Crystallization of Turning Rollers' Massive Castings: Development and Analysis. International Journal of Mineral Processing and Extractive Metallurgy, 2 (3), 34–39. doi: https://doi.org/10.11648/j.ijmpem.20170203.12
20. Abbas, M., ElMaraghy, H. (2016). Functional Synthesis of Manufacturing Systems Using Co-platforming. Procedia CIRP, 52, 102–107. doi: https://doi.org/10.1016/j.procir.2016.07.069
21. Tsybulkin, G. A. (2017). Synthesis of structure of system for self-regulation of electrode melting rate. The Paton Welding Journal, 2017 (7), 2–5. doi: https://doi.org/10.15407/tpwj2017.07.01
22. Guarino, P. (2016). The Universal Type Structure with Unawareness for Conditional Probability Systems. SSRN Electronic Journal. doi: https://doi.org/10.2139/ssrn.3069468
23. Onodera, A. N., Gavião Neto, W. P., Roveri, M. I., Oliveira, W. R., Sacco, I. C. (2017). Immediate effects of EVA midsole resilience and upper shoe structure on running biomechanics: a machine learning approach. PeerJ, 5, e3026. doi: https://doi.org/10.7717/peerj.3026
24. Tsao, Y.-C. (2017). Channel coordination under two-level trade credits and demand uncertainty. Applied Mathematical Modelling, 52, 160–173. doi: https://doi.org/10.1016/j.apm.2017.07.046
25. Kohler, T., Froeschl, J., Bertram, C., Buecherl, D., Herzog, H.-G. (2010). Approach of a Predictive, Cybernetic Power Distribution Management. World Electric Vehicle Journal, 4 (1), 22–30. doi: https://doi.org/10.3390/wevj4010022
26. Kobylin, P. O. (2017). Functional and component structure of the population trading servicesystem. Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriya: Heolohiya. Heohrafiya. Ekolohiya, 46, 92–100. doi: https://doi.org/10.26565/2410-7360-2017-46-13
27. Assimakopoulos, N. A., Dimitriou, N. K., Theocharopoulos, I. C. (2010). Business intelligence systems for Virtual Enterprises: a cybernetic approach. International Journal of Applied Systemic Studies, 3 (4), 374. doi: https://doi.org/10.1504/ijass.2010.038349
28. Lutsenko, I., Fomovskaya, E., Vikhrova, E., Serdiuk, O. (2016). Development of system operations models hierarchy on the aggregating sign of system mechanisms. Eastern-European Journal of Enterprise Technologies, 3 (2 (81)), 39–46. doi: https://doi.org/10.15587/1729-4061.2016.71494
29. Lutsenko, I., Fomovskaya, E. (2015). Identification of target system operations. The practice of determining the optimal control. Eastern-European Journal of Enterprise Technologies, 6 (2 (78)), 30–36. doi: https://doi.org/10.15587/1729-4061.2015.54432
30. Lutsenko, I. (2015). Classification of systems and system entities. Metallurgical and Mining Industry, 12, 12–17.
31. Krasovskiy, A. A. (Ed.) (1987). Spravochnik po teorii avtomaticheskogo upravleniya. Moscow, 712.
32. Zaloga, V. A., Nagorniy, V. M., Nagorniy, V. V. (2016). Kontrol' dinamicheskogo sostoyaniya metalloobrabatyvayushchey tekhnologicheskoy sistemy i prognozirovanie ee resursa. Sumy: Sumskiy gosudarstvennyy universitet, 242.
33. Lutsenko, I., Fomovskaya, E. (1973). Synthesis of cybernetic structure of optimal spooler. Metallurgical and Mining Industry, 9, 297–301.
34. Mihaylov, V. V. (1973). Nadezhnost' elektrosnabzheniya promyshlennyh predpriyatiy. Moscow, 167.
35. Lutsenko, I. A. (2005). Developing a General Control Criterion for Complex Systems. Cybernetics and Systems Analysis, 41 (5), 789–792. doi: https://doi.org/10.1007/s10559-006-0016-4
36. Lutsenko, I., Fomovskaya, E., Oksanych, I., Serdiuk, O. (2017). Development of criterion verification method for optimization of operational processes with the distributed parameters. Radio Electronics, Computer Science, Control, 3, 161–174. doi: https://doi.org/10.15588/1607-3274-2017-3-18
37. Lutsenko, I., Fomovskaya, E., Oksanych, I., Vikhrova, E., Serdiuk, O. (2017). Formal signs determination of efficiency assessment indicators for the operation with the distributed parameters. Eastern-European Journal of Enterprise Technologies, 1 (4 (85)), 24–30. doi: https://doi.org/10.15587/1729-4061.2017.91025

38. Lutsenko, I., Fomovskaya, E., Oksanych, I., Koval, S., Serdiuk, O. (2017). Development of a verification method of estimated indicators for their use as an optimization criterion. Eastern-European Journal of Enterprise Technologies, 2 (4 (86)), 17–23. doi: https://doi.org/10.15587/1729-4061.2017.95914
39. Lutsenko, I., Fomovskaya, O., Vihrova, E., Serdiuk, O., Fomovsky, F. (2018). Development of test operations with different duration in order to improve verification quality of effectiveness formula. Eastern-European Journal of Enterprise Technologies, 1 (4 (91)), 42–49. doi: https://doi.org/10.15587/1729-4061.2018.121810
40. Lutsenko, I., Oksanych, I., Shevchenko, I., Karabut, N. (2018). Development of the method for modeling operational processes for tasks related to decision making. Eastern-European Journal of Enterprise Technologies, 2 (4 (92)), 26–32. doi: https://doi.org/10.15587/1729-4061.2018.126446
41. Lutsenko, I., Fomovskaya, E., Koval, S., Serdiuk, O. (2017). Development of the method of quasi-optimal robust control for periodic operational processes. Eastern-European Journal of Enterprise Technologies, 4 (2 (88)), 52–60. doi: https://doi.org/10.15587/1729-4061.2017.107542
42. DualSystem. Available at: https://www.dropbox.com/s/nf1a5eckk5vtxqb/DualSystem.xls?dl=0

DOI: 10.15587/1729-4061.2018.150805

IMPROVING EFFICIENCY FOR ENSURING DATA GROUP ANONYMITY BY DEVELOPING AN INFORMATION TECHNOLOGY (p. 41-56)

Oleg Chertov
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0003-0087-1028

Dan Tavrov
Private Institution "University
"Kyiv School of Economics"", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0002-3689-2931

Widespread introduction of methods that ensure anonymity of information about individual groups (teams) of respondents in the field of official statistics is restrained by the lack of relevant industrial information technologies and systems. A three-level client-server architecture of an information technology providing data group anonymity was provided in which clients, application servers and databases are united into a local network to enhance security of primary data. A conceptual data model covering all key components of group anonymity was described. Implementation of the technology based on the Java Enterprise Edition 8 platform, Oracle GlassFish Server application server, MySQL database server and SciLab engineering calculations system wase considered.

The information technology enables providing of group anonymity of data in the event of a threat of its violation by analyzing data of an auxiliary microfile. The technology provides operations for constructing fuzzy group models using a genetic algorithm and modification of a microfile with the help of a mimetic algorithm which enables effective providing of anonymity by introducing minor insignificant distortions into data.

Application of the technology was illustrated by solution of the task of providing anonymity of a military group based on real data of American Community Survey, 2013. It was shown that solving the problem by a team of five specialists has enabled at least two and a half times faster the process of preparation of a microfile than by the use of an existing technology.

Keywords: information technology, group anonymity, microfile, fuzzy model, evolutionary algorithm.

References

1. Duncan, G. T., Elliot, M., Salazar-González, J.-J. (2011). Statistical Confidentiality. Principles and Practice. Springer-Verlag, 212. doi: https://doi.org/10.1007/978-1-4419-7802-8
2. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, Version v0.34. Available at: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
3. Chertov, O. R., Tavrov, D. Y. (2017). Providing group anonymity as a part of CSID data process. Shtuchnyi intelekt, 3-4, 127–138.
4. Chertov, O., Tavrov, D. (2017). Improving efficiency of providing data group anonymity by automating data modification quality evaluation. Eastern-European Journal of Enterprise Technologies, 5 (4 (89)), 31–39. doi: https://doi.org/10.15587/1729-4061.2017.113046
5. Chertov, O., Tavrov, D. (2014). Microfiles as a Potential Source of Confidential Information Leakage. Studies in Computational Intelligence, 87–114. doi: https://doi.org/10.1007/978-3-319-08624-8_4
6. Tavrov, D., Chertov, O. (2016). Evolutionary approach to violating group anonymity using third-party data. SpringerPlus, 5 (1). doi: https://doi.org/10.1186/s40064-016-1692-9
7. Butz, M. V. (2015). Learning Classifier Systems. Springer Handbook of Computational Intelligence, 961–981. doi: https://doi.org/10.1007/978-3-662-43505-2_47
8. Holland, J. H. (1975). Adaptation in Natural and Artificial Systems. Ann Arbor, MI: University of Michigan Press, 183.
9. Valenzuela-Rendón, M. (1991). The Fuzzy Classifier System: Motivations and First Results. Proceedings of Parallel Solving from Nature (PPSN II), 330–334.
10. Smith, S. F. (1980). A Learning System Based on Genetic Adaptive Algorithms. Pittsburgh: University of Pittsburgh, 214.
11. Carmona, C. J., González, P., del Jesus, M. J., Herrera, F. (2014). Overview on evolutionary subgroup discovery: analysis of the suitability and potential of the search performed by evolutionary algorithms. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 4 (2), 87–103. doi: https://doi.org/10.1002/widm.1118
12. Ishibuchi, H., Nakashima, T., Murata, T. (1999). Performance evaluation of fuzzy classifier systems for multidimensional pattern classification problems. IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics), 29 (5), 601–618. doi: https://doi.org/10.1109/3477.790443

13. Hundepool, A., de Wolf, P.-P., Bakker, J., Reedijk, A., Franconi, L. et. al. (2018). μ-ARGUS Version 5.1.3. User's Manual. Available at: http://neon.vb.cbs.nl/casc/Software/MUmanual5.1.3.pdf
14. Angiuli, O., Waldo, J. (2016). Statistical Tradeoffs between Generalization and Suppression in the De-identification of Large-Scale Data Sets. 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). doi: https://doi.org/10.1109/compsac.2016.198
15. Sweeney, L. (2002). K-Anonymity: A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10 (05), 557–570. doi: https://doi.org/10.1142/s0218488502001648
16. Fienberg, S., McIntyre, J. (2005). Data Swapping: Variations on a Theme by Dalenius and Reiss. Journal of Official Statistics, 21 (2), 309–323.
17. Evfimievski, A. (2002). Randomization in privacy preserving data mining. ACM SIGKDD Explorations Newsletter, 4 (2), 43–48. doi: https://doi.org/10.1145/772862.772869
18. Templ, M. (2008). Statistical Disclosure Control for Microdata Using the R-package sdcMicro. Transactions on Data Privacy, 1 (2), 67–85.
19. Domingo-Ferrer, J., Mateo-Sanz, J. M. (2002). Practical data-oriented microaggregation for statistical disclosure control. IEEE Transactions on Knowledge and Data Engineering, 14 (1), 189–201. doi: https://doi.org/10.1109/69.979982
20. Chertov, O. R. (2012). Minimizatsiya spotvoren pry formuvanni mikrofailu z zamaskovanymy danymy. Visnyk Skhidnoukrainskoho natsionalnoho universytetu im. V. Dalia, 8 (179), 240–246.
21. Chertov, O., Tavrov, D. (2012). Providing Group Anonymity Using Wavelet Transform. Lecture Notes in Computer Science, 25–36. doi: https://doi.org/10.1007/978-3-642-25704-9_5
22. Chertov, O., Tavrov, D. (2016). Two-Phase Memetic Modifying Transformation for Solving the Task of Providing Group Anonymity. Studies in Fuzziness and Soft Computing, 239–253. doi: https://doi.org/10.1007/978-3-319-32229-2_17
23. Zadeh, L. A. (2013). Toward a restriction-centered theory of truth and meaning (RCT). Information Sciences, 248, 1–14. doi: https://doi.org/10.1016/j.ins.2013.06.003
24. Neri, F., Cotta, C. (2012). A Primer on Memetic Algorithms. Studies in Computational Intelligence, 43–52. doi: https://doi.org/10.1007/978-3-642-23247-3_4
25. Goldberg, D. E., Korb, B., Deb, K. (1989). Messy Genetic Algorithms: Motivation, Analysis, and First Results. Complex Systems, 3, 493–530.
26. Syswerda, G. (1991). Schedule Optimization Using Genetic Algorithms. Handbook of Genetic Algorithms. New York: Van Nostrand Reinhold, 332–349.
27. Eiben, A. E., Smith, J. E. (2015). Introduction to Evolutionary Computing. Springer-Verlag, 287. doi: https://doi.org/10.1007/978-3-662-44874-8
28. Brindle, A. (1981). Genetic Algorithms for Function Optimization. Edmonton: University of Alberta, 193.
29. Zadeh, L. A. (1975). The concept of a linguistic variable and its application to approximate reasoning – I. Information Sciences, 8 (3), 199–249. doi: https://doi.org/10.1016/0020-0255(75)90036-5
30. Wrobel, S. (1997). An algorithm for multi-relational discovery of subgroups. Lecture Notes in Computer Science, 78–87. doi: https://doi.org/10.1007/3-540-63223-9_108
31. Lavrač, N., Flach, P., Zupan, B. (1999). Rule Evaluation Measures: A Unifying View. Lecture Notes in Computer Science, 174–185. doi: https://doi.org/10.1007/3-540-48751-4_17
32. Ishibuchi, H., Nozaki, K., Yamamoto, N., Tanaka, H. (1995). Selecting fuzzy if-then rules for classification problems using genetic algorithms. IEEE Transactions on Fuzzy Systems, 3 (3), 260–270. doi: https://doi.org/10.1109/91.413232
33. Syswerda, G. (1989). Uniform Crossover in Genetic Algorithms. Proceedings of the 3rd International Conference on Genetic Algorithms. Morgan Kaufmann Publishers Inc., 2–9.
34. Olivetti, E., Greiner, S., Avesani, P. (2014). Statistical independence for the evaluation of classifier-based diagnosis. Brain Informatics, 2 (1), 13–19. doi: https://doi.org/10.1007/s40708-014-0007-6
35. Ruggles, S., Flood, S., Goeken, R., Grover, J., Meyer, E., Pacas, J., Sobek, M. (2018). Integrated Public Use Microdata Series, Version 8.0 [Dataset]. Minneapolis: University of Minnesota. Available at: https://usa.ipums.org/usa/
36. 2011 Demographics. Profile of the Military Community (2012). Available at: http://www.militaryonesource.mil/12038/MOS/Reports/2011_Demographics_Report.pdf