«CHALLENGES AND THREATS TO CRITICAL INFRASTRUCTURE»

Detroit (Michigan, USA) - 2023

Challenges and threats to critical infrastructure. Collective monograph - NGO Institute for Cyberspace Research (Detroit, Michigan, USA), 2023. - 325 p.

The collective monograph was prepared by ukranian scholars within the framework of studies of a wide range of security issues. The authors of the monograph look at the problems of security of the state`s security in a rich manner behind such basic warehouses as military security, information security, military-technical security, environmental and technogenic security

Reviewers:

Ponomarev S.P. - Doctor of Jurisprudence, head of the Department of Administration of the State Service of Special Communications and Information Protection of Ukraine

Hnatyuk S.O. - Ph.D. Chief Researcher of the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection

Silvestrov A.M. - Ph.D. Prof. National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

ISBN-10/979-8-218-22315-1

Authors

Chapter 1. Avramenko O.V., Polishchuk V.V., Sarapin Yu.O., Voinov I.A. 1, V.A. Malik, N.V. Zhenyuk, N.I. Voropai, O.G. Korol, A.Yu. Strelnikova, Yu.V. Kostenko, O.V. Peredrii, V.V. Gordiychuk, Grinenko O.I., Hrytsyuk V.V., Zubkov V.P., Ptashkin R.L., Palagin V.V., Savostyanenko M.V., Klymenko K.V., Klymenko K.V., Tyutyunyk V . ., Kapelushna T.V.

Chapter 2. Azarenko O., Honcharenko Yu., Divizinyuk M., Shevchenko R., Shevchenko O., V.M. Vashchenko, V.I. Skalozubov, I.B. Korduba, Shcherbak O., Khmyrova A., Khrystych V., Zhuk V. M., Pohosyan G. A., Yevlanov M. V., Cherepnyov I. A., Chumachenko S. M., Kolomiets D. P., Matsko P. I., Kaplia I. O., Romanyuk V. P., Medvedev M. G., Mulyava O. M., Peredrii O. V., Komisarov M. V., Proshchyn I. V., Sydorenko V .L., Eremenko S.A., Tyshchenko V.O., Vlasenko E.A., Pruskyi A.V., Demkiv A.M., Yudina D.O.

Chapter 3. V. N. Yelisieiev, E. V. Bykova, V. S. Tyshchenko, N. V. Zaika, V. A. Popel, S. S. Chumachenko, O. V. Ivchenko, V. V. Palagin, R. Kyrychok. V., Laptev O.A., Laptev S.O., Sobchuk A.V., Ponomarenko V.V., Barabash A.O., Murasov R.K., Chumachenko S.M., Sirik A.O. , Yevtushenko O.V., Sobchuk V.V., Pichkur V.V., Lapteva T.O., Kopytko S.B.

Chapter 4. Goncharenko I.O., Kuchma T.L., Prodanyuk D.M., Zaretskyi I.S., Karpenko M.I., Moshenskyi A.O., Derman V.A., Khoperskyi S. V., Chumachenko S.M., Ponomarenko S.O., Popel V.A, Maslennikova T.A.

Chapter 5. Vovchuk T., Shevchenko R., Shevchenko O., Guida O.G., Kiselyov V.B., Ometsynska N.V., Trysnyuk T.V., Konetska O.O., Nagornyi E. I., Marushchak V.M., Volynets T.V., Prystupa V.V., Trofimchuk O.M., Trysnyuk V.M., Shumeiko V.O., Chumachenko S.M., Lysenko O.I. , O. M. Tachynina, O. V. Furtat, S. O. Furtat, I. O. Sushin.

Chapter 6. Viola Vambol, Alina Kowalczyk-Juśko, Sergij Vambol, Nadeem Ahmad Khan, Aaron Dumont, Zaporozhchenko M.M., Legominova S.V., Muzhanova T.M., Ometsynska N.V., Kiselyov V. B., Huida O. G., Shchavinskyi Y.V., Palchynska V.B.

Chapter 7. Altaf Hussain Lahori, Barbara Savytska, Parisa Ziarati, Barbara Krokhmal-Marchak, Niloofar Mozaffari, Nastaran Mozaffari, Miasoyedova A., Divizinyuk M., Shevchenko R., Myroshnychenko A., Aldoshin O.O., Kalinovsky A.Ya., Vykhvatin M.V., Havrys A.P., R.S. Yakovchuk, O.O. Pekarska, M.V. Yevlanov, R.V. Antoshchenkov, I.A. Cherepnyov, I.I. Kravchenko, V. Loik. B., Synelnikov O.D., Goncharenko M.O., Nazarenko S.Yu., Mandrychenko D.S., Shapovalov M.M., Pichugin M.A., Vynogradov S.A., Samchenko T.V. , Nuyanzin O.V., Sverchkov O.V., Faure E.V., Skutskyi A.B., Lavdanskyi A.O., Grechanyk O.S., Shakhov S.M., Zinchenko O.O., Yatsenko V.O., Vambol S.O.

Chapter 8. Adamova G.V., Anila Kausar, Ambreen Afza, Altaf Hussain Lahori, Bobkov Y.V., Shevchuk A.A., Stamati V.G., Vynogradov S.A., Chumachenko S.M., Lysenko O.I., Novikov V.I., Furtat O.V., Furtat S.O., Sushin I.O., Pisnya L.A., Mishchenko I.V., Vambol S.O., Vambol Viola

Chapter 9. Yakovliev Ye.O., Rudko G.I., Yermakov V.M., Chumachenko S.M., Kodryk A.I., Dyatel O.O., Lubenska N.O.

CONTENT

УДК 004.056

10.ПІДХОДИ ДО ПОБУДОВИ ЗАВАДОСТІЙКОГО ПЕРЕСТАНОВОЧНОГО КОДУ ДЛЯ НЕРОЗДІЛЬНОГО ФАКТОРІАЛЬНОГО КОДУВАННЯ ДАНИХ

Фауре Е.В.[1], Махинько М.В.[2]
1 Черкаський державний технологічний університет, Черкаси, Україна
ГО «Інститут дослідження кіберпростору»
2 GoodLabs Studio Inc., Toronto, ON M5H 3E5, Canada
E-mail: e.faure@chdtu.edu.ua

Approaches to construct error-correcting permutation code for non-separable factorial data coding

The report highlights approaches to construct error-correcting permutation code in the context of its use in integrated data protection systems against channel errors and unauthorized access based on non-separable factorial coding. The use of affine and projective general linear groups to form an ensemble of permutations, in addition to providing a given code distance for permutation dictionaries (arrays), allows generating network and session keys during secure data exchange. The statistical approach to construct permutation code is based on enumerating permutations and selecting those permutations, which distance does not exceed a given value to all previously selected codewords.

Передавання коротких пакетів є ключовою особливістю сучасних бездротових систем, наднадійних і сенсорних мереж, масових комунікацій машинного типу (МТС), IoT застосувань. Поширеність таких систем і мереж у сучасному світі вимагає створення нових і адаптацію існуючих підходів до забезпечення цілісності та конфіденційності переданої інформації. Зокрема, потужність необхідних ресурсів для канального кодування та криптографічного захисту, а також їх швидкодія відіграють подекуди визначальну роль.

Ця робота розглядає підходи до побудови завадостійких перестановочних кодів [1, 2] у контексті використання їх у системах інтегрованого захисту інформації від помилок каналу зв'язку та несанкціонованого доступу на основі нероздільного факторіального кодування даних [3, 4]. Такі перестановочні коди можуть бути використані, зокрема, з метою формування ансамблю кодових символів факторіального коду для інформаційної взаємодії об'єктів МТС з динамічно змінюваною структурою, а також забезпечення надійного передавання перестановок у складних завадових умовах, утому числі, для трьохетапного криптографічного протоколу на основі перестановок [5].

Множину перестановок на Z_M будемо називати масивом перестановок [6] і позначати через S_M. Відстань між перестановками $\pi_i, \pi_j \in S_M$ будемо позначати

через D_{ij}. Тоді завадостійким перестановочним кодом є (M, D_{min}) є код, утворений підмножиною перестановок масиву S_M, де попарна відстань між перестановками π_i, π_j цієї підмножини задовольняє нерівності $D_{ij} \geq D_{min}$. Потужність коду (M, D_{min}) позначимо через $N(M, D_{min})$.

Спершу розглянемо алгоритми формування кодів $(M, M-1)$ і $(M+1, M-1)$ з простим M для досягнення $N(M, M-1) = M(M-1)$ і $N(M+1, M-1) = (M+1)M(M-1)$.

Код $(M, M-1)$ утворюється афінною загальною лінійною групою $AGL(1, M) = \{ax + b | a, b, x \in GF(M), a \neq 0\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду, тобто якщо $S_M = \{ax + b, a, b \in Z_M, a \neq 0\}$ і $\sigma \in S_M$, то $\{a\sigma_x + b, a, b \in Z_M, a \neq 0\} = S_M$.

Код $(M+1, M-1)$ утворюється проективною загальною лінійною групою $PGL(2, M) = \left\{ f(x) = \frac{ax+b}{cx+d} \middle| a, b, c, d \in GF(M), x \in GF(M) \bigcup \infty, ad \neq bc \right\}$ [6] і з простим M породжується будь-яким елементом (перестановкою) цього коду, тобто якщо $S_{M+1} = \left\{ f(x) = \frac{ax+b}{cx+d} \middle| a, b, c, d \in Z_M, x \in Z_M \bigcup \infty, ad \neq bc \right\}$ і $\sigma \in S_{M+1}$, то $\left\{ f(x) = \frac{a\sigma_x + b}{c\sigma_x + d} \middle| a, b, c, d \in Z_M, ad \neq bc \right\} = S_{M+1}$.

Застосування афінної та проективної загальної лінійної груп для формування алфавіту повідомлень (перестановок), окрім забезпечення кодової відстані $M-1$ для словників (масивів) перестановок S_M і S_{M+1}, дозволяє формувати мережні та сеансові ключі під час захищеного обміну даними.

Статистичний підхід [7] до формування (M, D_{min})-коду та оцінювання його потужності $N(M, D_{min})$ базується на переборі множини перестановок $\{\pi\}$ довжини M і відбору тих перестановок, відстань від яких не перевищує значення D_{min} до всіх відібраних до цього кодових слів.

Для забезпечення можливості побудови коду (M, D_{min}) за значень M, для яких реалізувати практично формування $M!$ перестановок неможливо, початкова множина перестановок представляє собою деяку власну підмножину потужності N_{lim} повної множини з $M!$ перестановок.

Експериментально визначені залежності середнього та максимального значень потужності $N(M, D_{min}, N_{lim})$ коду (M, D_{min}), утвореного за підмножиною

з N_{lim} перестановок, від значення N_{lim}, а також методика побудови апроксимаційних квадратичних поліномів для визначених залежностей можуть бути використані для екстраполяції цих залежностей і прогнозування їх поведінки.

Література

1. Blake I. Permutation codes for discrete channels / I. Blake // IEEE Trans. Inf. Theory. – 1974. – Issue 20, No. 1. – P. 138–140.
2. Smith D. H. A new table of permutation codes / D. H. Smith, R. Montemanni // Des. Codes Cryptogr. – 2012. – Issue 63, No 2. – P. 241–253.
3. Faure E. V. Factorial coding with data recovery / E. V. Faure // Visnyk Cherkaskogo Derzhavnogo Tehnol. Univ. – 2016. – No. 2. – P. 33–39.
4. Faure E. V. Factorial coding with error correction / E. V. Faure // Radio Electron. Comput. Sci. Control. – 2017. – Issue 3. – P. 130–138.
5. Shcherba A. Three-Pass Cryptographic Protocol Based on Permutations / A. Shcherba, E. Faure, O. Lavdanska // 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT). – Kyiv, Ukraine : IEEE, 2020.
6. Mojica de la Vega L. G. Permutation Arrays with Large Hamming Distance / L. G. Mojica de la Vega. – The University of Texas at Dallas, 2017. – 106 p.
7. Faure E. Permutation-Based Block Code for Short Packet Communication Systems / E. Faure, A. Shcherba, M. Makhynko, B. Stupka, J. Nikodem, R. Shevchuk // Sensors. – 2022. – Issue. 22, No. 14, 5391.

УДК 336.74

11.АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Хохлачова Ю. Є.[1], Гаврилова А. А.[2]

1 Національний авіаційний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

2 Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

E-mail: yuliiahohlachova@gmail.com, sharaya1972@gmail.com

Analysis of information security threats in modern information and communication systems and networks

Threats to information security and the consequences of their implementation in the form of cyberattacks were analyzed, and attractive directions for cybercriminals by sphere of activity were clarified. The dynamics of changes in the activity of cybercriminals are considered. As a result, it