Міністерство освіти і науки України
Одеський національний технологічний університет
Інститут комп`ютерної інженерії, автоматизації, робототехніки та програмування ім.П.Н.Платонова

«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І АВТОМАТИЗАЦІЯ – 2023»

МАТЕРІАЛИ
XVI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

19 - 20 ЖОВТНЯ 2023 р.

м.ОДЕСА

ЗМІСТ
CONTENT

точність розрахунків для методу умовної оптимізації в довірчій області. Виходячи з цього, можна припустити, що точність інших методів становить приблизно 0,00001.

```
k1: 0   k2: 0   k3: 1   p:0.5   q:0.5   P: 0.21875
Максимальна ймовірність методом градієнтного спуску: 0.343551
Оптимальне q: 0.264911
Кількість ітерацій: 4
Час виконання алгоритму: 0.005000 с.
Максимальна ймовірність симплекс-методом Nealder-Mead: 0.343551
Оптимальне q: 0.264941
Кількість ітерацій: 14
Час виконання алгоритму: 0.000999 с.
Максимальна ймовірність методом Powell: 0.343551
Оптимальне q: 0.264913
Кількість ітерацій: 2
Час виконання алгоритму: 0.002001 с.
Максимальна ймовірність методом спряжених градієнтів CG: 0.343551
Оптимальне q: 0.264911
Кількість ітерацій: 1
Час виконання алгоритму: 0.001999 с.
Максимальна ймовірність методом BFGS (Бройдена-Флетчера-Голдфарба-Шанно): 0.343551
Оптимальне q: 0.264911
Кількість ітерацій: 5
Час виконання алгоритму: 0.001000 с.
Максимальна ймовірність методом L-BFGS-B: 0.343551
Оптимальне q: 0.264911
Кількість ітерацій: 4
Час виконання алгоритму: 0.002000 с.
Максимальна ймовірність усіченим методом Ньютона TNC: 0.343551
Оптимальне q: 0.264911
Кількість ітерацій: 4
Час виконання алгоритму: 0.002000 с.
Максимальна ймовірність послідовним методом найменших квадратів SLSQP: 0.343551
Оптимальне q: 0.264936
Кількість ітерацій: 5
Час виконання алгоритму: 0.001000 с.
Максимальна ймовірність методом умовної оптимізації в довірчій області trust-constr: 0.343551
Оптимальне q: 0.264922
Кількість ітерацій: 13
Час виконання алгоритму: 0.032035 с.
Точність розрахунків: 0.000032
```

Рисунок 1 – Результати розрахунків іншими методами

Результатами роботи є прототип програми для розрахунку значення параметра q, при якому досягається максимальна ймовірність виникнення одночасної появи трьох подій за схемою Бернуллі. Наведено час виконання кожного із застосованих алгоритмів. Також наведена точність розрахунків для методу умовної оптимізації в довірчій області.

Список використаної літератури

[1] Донченко В. С., Сидоров М. В.-С. Теорія ймовірностей та математична статистика для соціальних наук: навч. посібник. – К. : ВПЦ "Київський університет", 2015.

[2] Масол В. И. О распределении некоторых статистик (0, 1)-вектора. Исследование операций и АСУ. 1987. Вып. 29.

[3] Масол В. И., Поперешняк С. В. Проверка случайности расположения битов в локальных участках (0, 1)-последовательности. Кибернетика и системный анализ. 2020. Т. 56. №3.

[4] Теслюк В.М. Градієнтні методи розв'язання оптимізаційних задач: Ч.3. Конспект лекцій з курсу "Методи синтезу та оптимізації" для студентів базового напрямку "Комп'ютерні науки". – Львів: Самвидав кафедри САП Національного університету "Львівська політехніка". 2013.

УДК 004.056.55

SIMULATION OF A CRYPTOGRAPHIC PROTOCOL FOR AGREEMENT A SHARED SECRET KEY-PERMUTATION OF SIGNIFICANT DIMENSION WITH ITS ISOMORPHIC REPRESENTATIONS

Krasilenko V. G., Kiporenko S. S., Chikov I. A., Nikitovych D. V. (krasvg@i.ua, kiporenko@vsau.vin.ua, ilya95chikov@gmail.com, diananikitovych@gmail.com)
Vinnytsia National Agrarian University, Vinnytsia National Technical University (Ukraine)

Abstract

A protocol for agreement by user parties of secret keys-permutations of significant dimension and their new isomorphic matrix representations is proposed. Features and advantages of such representations are considered. The need to create such secret permutation keys to improve the

cryptographic stability of matrix affine-permutation ciphers and other cryptosystems of the new matrix type is well-founded. The results of modeling the basic procedures of the proposed key agreement protocol in the form of an isomorphic permutation of a significant dimension, namely the processes of generating permutation matrices and their degrees, are given. Model experiments of the protocol as a whole, including accelerated methods of raising permutations to significant degrees, were performed. Such methods use sets of fixed permutation matrices, which are degrees of the underlying permutation matrix, and all these matrices are given in their isomorphic representations. The values of the fixed exponents correspond to the corresponding weights of the digits of the binary or other code representations of the selected random numbers. The results of simulation modeling demonstrated the adequacy and advantages of isomorphic representations of the processes of functioning of matrix-algebraic models of cryptographic transformations and the proposed secret key-permutation agreement protocol.

Keywords

matrix-algebraic model, matrix representations, isomorphic permutation key, cryptogram, cryptographic transformations, affine-permutation cipher, protocol, matrix-type cryptosystem.

1. Introduction, overview and analysis of publications

Introduction. Generalization of known cryptosystems [1-3], with scalar-type data formats to the cases of matrix-tensor formats, emergence and research of a new class of matrix-type cryptosystems (MTC) [4-7], based on their matrix-algebraic models (MAM) of cryptographic transformations (CT) 2D (3D) - arrays, images (Is), which have a number of significant advantages, contributed to the intensification of MTC, MAM research and the demonstration of a number of new improvements and applications [7-12], MAMs in their hardware implementations are more easily displayed on matrix processors, have extended functionality, improved crypto-resistance, allow checking the integrity of cryptograms of black and white, color images [8], and the presence of distortions in them [7], create block ones [9], parametric [9], multi-page [10] models with their significant stability [11]. Secret key generation protocols for such ciphers were partially considered in works [13-15], including in works [14], [15] some matrix modifications of known key agreement protocols were proposed. Generalized MAM, matrix affine and affine-permutation ciphers (MAPCs), their modifications were studied and used in the creation of blind and other improved digital signatures in [11]. For CT in matrix models of permutations (MM_P), with their basic procedures of matrix multiplication and some other element-by-element modulo operations on matrices, byte matrices formed from rows, columns, vectors, which in unitary or other codes display symbols, codes, bytes, must be multiplied by the permutation matrix (PM). Procedures for rearranging bits, bytes or their groups are the most common and mandatory for almost all known and newly created algorithms and ciphers. To increase the entropy of cryptograms images with their CT based on MM_P and change their histograms, the decomposition of R, G, B components and their bit slices and several matrix keys (MKs) of the PM type are necessary [6], [7], [10]. A number of such pseudo-random (current, step-by-step, frame-by-frame) MKs, which would meet the requirements and be quickly generated, is also needed for masking, CT of video files or stream of blocks from files, images with their significant sizes.

Formulation of the problem. Thus, there is a need for the MAM to form a number of MKs of the PM-type that would satisfy a number of requirements from the main MK. Since the issue of matching the main MK (MMK) of a general type, but not the sequence of PMs, was considered in [14], [15], and the methods of generating a stream of MKs-permutations from the main MK were partially considered in [16], but only for bit MPs of small sizes (256*256), then the purpose of the work is to propose and investigate a protocol for the coordination of a secret (main) MK in the form of an PM of significant dimensions, i.e., an main PM (MPM), to improve and adapt the type and structure of a MPM of such or even greater dimensions to the images format and to fast hardware solutions, to model this protocol and the process of formation flow of PMs from such a MPM for MAM CT in MT systems. In addition, the above review and analysis of publications allows to determine another important task, namely the need to develop and model such MAM CTs, which would be best suited for implementation based on vector-matrix multipliers (VMMs), as well as to determine the characteristics and indicators of such models and implementations.

2. Presentation of the main material and research results

An overview of MT ciphers, especially multifunctional parametric block ciphers [9], their analysis shows that it is advisable to use isomorphism of various representations of permutations (matrices or vectors) that act as a master key (MK) and block or step-by-step, round MKs to achieve the goal of PM-type, i.e. sub-keys (SKs), which are matrices of permutations of P (its powers!) or vectors isomorphic to them. It is known from the works [7], [9-11] that with CT based on the basis of matrix affine-permutation ciphers (MAPCs) and vector affine-permutation ciphers (VAPCs), cryptograms for some types of text-graphic documents (TGD) and images (I), especially for block-based MAMs, when using one personal computer (PC) for all blocks are insufficient in terms of stability, however, a number of PCs created from MPM solve this problem. And that is why the aspect of coordinating the secret MPM of the PM-type with a significant dimension is important. Let's consider the situation when for M blocks with a length of 256*256 bytes, presented in the form of a matrix of a black and white image, it is necessary to rearrange all bytes in accordance with PM. In this case, PM in the generally accepted form should be square with N*N elements ("0" or "1"), where $N=2^{16}=65536$. The power of the set of possible such PMs, i.e. their number, is estimated as N!=65536!, which gives colossal values for this N. But each byte address of the block can be represented by two bytes indicating two coordinates (row and column) of the block. This gives us the opportunity to represent any permutation with two blocks (256*256 elements) of bytes, setting in each identical address of these blocks the corresponding senior byte (in the first block) and junior byte (in the second block) coordinates of the new address of the byte selected for permutation. The view of the software module in Mathcad for generating the basic (main) MK (PM) and the view of its components KeyA and KeyB in the format of two images is shown in report. Therefore, any PM can be uniquely represented by two matrices of size 256*256, the elements of which take values from the range 0-255, with the peculiarity that each of their 256 gradations of intensity in each of these two matrices (images) is repeated exactly 256 times. The histograms of KeyA and KeyB PM components have the form of horizontal lines. We note that such an isomorphic representation of the PM in the form of two images gives us the opportunity to use these components KeyA and KeyB as two secret MCs of a general type, for example, as additive and multiplicative keys in the MAPCs. This is evidenced by the simulation results of the CT image (Im) using in MAPC the proposed PM and its components, as keys, shown with the matrices of explicit image (Im), intermediates, its cryptograms (Cmap) and verifiable images [16]. And the histograms of the explicit image, its cryptograms after each CT with the affine components of this PM, induced in [16], will be shown in the report. These experiments confirmed that CT with the existing 2 components of the PM give high-quality cryptograms CD-ImAa and CD-ImAm, whose histograms H-Cda and H-CDm are so close to the uniform distribution law that even for image (Im) with an entropy of 0.738, the entropy of cryptograms differs from the theoretical maximum (8 bits) by just a fraction of a percent, going all the way up to 7.99. The simulation results of the multi-step MAPC [15] for different cases, when the components of affine transformations are first performed in a different sequence and with different MK from the PM, and then permutation using the PM also proved similar qualitative CTs, when applying the proposed representations of the PM. But for all modifications of the MAM with such PMs, the power of the set of which is estimated by a significant value N! = (256*256)!, the issue of agreeing session secret MPM is paramount. Let's consider the essence of the protocol of agreement of the MPM by the parties. Let there be sides: x (Alisa) and y (Bob). Let's assume that one PM is known from the set of admissible components in the form of KeyA and KeyB, shown in images. In addition, there is always a PM of reverse permutation, which for the selected representation has the form of 2 KeyAO and KeyBO. Each of the parties in the 1 step isomorphically elevates the MPM to their chosen secret degree (we have 11 and 17 for example!), sends a new PM to the other party, and in the 2 step, the party receives the new PMs similarly elevate them to the same random secret degrees. Here is an analogy with the Diffie-Hellman protocol. In report show Mathcad program modules, displaying the procedure of iterative permutations of the initial MPM, isomorphic to the elevation of the PM to the required power (11!) by side z (Alisa). Using similar modules, the other side also isomorphically calculates the PM, as initial MPM to required power (17!) by side y (Bob). New PMs received by the parties after the first step (each in the form of two of its components) are sent to the other party. The participants in the session, obtained by exchanging matrices, subject the parties to permutations of their elements chosen by the parties. In an isomorphic representation, this is equivalent to raising the permutation matrix to the appropriate power. After the second step the parties receive identical new PMs, i.e. essentially one secret PM. The modeling results of these two steps of the secret MK agreement protocol in Mathcad in form of intermediate

exchange and resulting secret MPMs in an isomorphic image representation will be presented. The parties do not know the degrees of the other party, but the MPs they received are identical, which is confirmed by simulation results. Thus, exponentiation of MPM (N*N bit matrices, where $N=2^{16}$!) is equivalently replaced by fast permutations, which, moreover, can be even more accelerated for significant powers by using some basic set of fixed degrees of MPM and their specific sequence, which provides significant advantages by accelerating the calculation of MPM degrees, simplifying possible implementations. In accordance with the MP protocol, values of significant dimensions must be multiplied many times, that is, raised to a power. And the degrees to which the parties raise these isomorphically presented MPs must be significant enough to ensure the necessary crypto-resistance against random attacks. Therefore, taking into account the necessity and expediency of using the above-mentioned accelerated methods of raising matrices to a power, we show an adequate isomorphic transformation of this procedure into some sequence of fixed permutations. Depending on the code in which the value of the degree is given, appropriate permutations are selected from the formed set of fixed MPs, the degrees of which correspond to the corresponding weights of the digits of the binary code. The results of these simulations, the corresponding formulas, procedures, key fragments will be given in the report. A comparison of the elements of the obtained matrices confirmed their complete correspondence and equality. The results obtained by modeling confirm the correctness of the protocol. Although the initial MPM is known to both parties, the protocol allows without knowledge of the secret degrees being chosen sides, form a secret key, PM in a similar isomorphic form in a time proportional to the number fixed permutations. In addition, stability analysis taking into account the power of the set formed by this the protocol of the relevant PM of significant dimensions showed the impossibility of carrying out attacks as a result of a huge set of possible MPs, which is estimated by the value (2^{16})!

3. Conclusions

A protocol for agreeing a secret key in the form of isomorphic representations of PMs of significant dimensions was proposed, model experiments were performed that confirmed the adequacy of the functioning of the models and the proposed protocol and methods of PM generation, their advantages. The models are simple, convenient, adaptable for various format and color images, implemented by matrix processors, have high efficiency, stability, and speed.

4. References

[1] Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Монографія І.Д. Горбенко. – Харків: Форт, 2012. – 878 с.

[2] Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.: іл.

[3] Digital masking using Mersenne matrices and its special images / A. Vostricov, M. Sergeev, N. Balonin, S. Chernyshev // Procedia Computer Science. 2017. Vol. 112. P. 1151-1159.

[4] Krasilenko V.G., Grabovlyak S.K. Matrix affine and permutation ciphers for encryption and decryption of images. Systems of information processing. - Kh., 2012. - Vol. 3 (101). - P. 53-62.

[5] X. Wu et al., “Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling,” Signal Process. 188, 108200 (2021).

[6] Krasilenko V.G., Dubchak V.M. Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling. Bulletin of Khm. National University. Technical sciences. - 2014. - No. 1. - pp. 74-79.

[7] Krasilenko V.G., Nikitovich D.V. Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity. Electronics and Information Technologies. - Lviv: National University, 2016. - Vo. 6. – pp. 111-127.

[8] Красиленко, В.Г., Огородник К.В., Флавицька Ю.А. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень. Комп’ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК– К., 2010. – С.120-124.

[9] Krasilenko V.G., Lazarev A.A, Nikitovich D.V. The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. Actual problems of information systems and technologies. 2020. P. 270-282.

[10] Krasilenko V.G., Lazarev A.A, Nikitovich D.V. Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In Control and Signal Processing Applications for Mobile and Aerial Robotic Systems. Hershey, PA: IGI Global, 2020. P. 170-214.

[11] Красиленко В.Г., Нікітович Д.В., Яцковська Р.О., Яцковський В.І. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису. Системи обробки інформації. – Х.: ХУПС імені Івана Кожедуба, 2019. – Вип. 1 (156). – С. 92-100.

[12] Лужецький В. Методи шифрування на основі перестановки блоків змінної довжини / В. Лужецький, І. Горбенко //Захист інформації. – 2015. – Т. 17, № 2. – С. 169-175.

[13] Квєтний Р.Н., Титарчук Є.О., Гуржій А.А. Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ЕССта RSA. Інформаційні технології та комп'ютерна інженерія. – 2016. – № 3. – С. 38-43.

[14] Красиленко В.Г., Нікітович Д.В. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу. Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

[15] Красиленко В.Г., Нікітович Д.В. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів. Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120.

[16] Krasilenko V.G., Nikitovich D.V. Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images. Abstracts of the II All-Ukrainian STC Computer Technologies: Innovations, Problems, Solutions. - Zhytomyr: Zhytomyr Polytechnic, 2019. - P. 67-77.

УДК 004.942

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ГОРІННЯ З УРАХУВАННЯМ НЕЛІНІЙНОСТІ ПРОЦЕСІВ

Кривченко Ю.В., Кривченко А.А.
(yuriikryvchenko@otfk.ukr.education, Nastya.otk.2014@gmail.com)
ВСП "Одеський технічний фаховий коледж ОНТУ" (Україна)

Пропонується розглядати математичні моделі горіння і вибухових процесів, зокрема автотурбулізацію полум'я, через еволюцію динамічної системи у фазовому просторі збурень. Розглянуто вплив на горіння таких важливих стабілізуючих факторів, як в'язкості стисливості середовища, збурення тиску і складових швидкості полум'я. Проведено комп'ютерне моделювання горіння з урахуванням нелінійності процесів методом тривимірних перетинів Пуанкаре та визначено параметри відповідних атракторів.

Побудова математичних моделей вибухових процесів і потенційно вибухонебезпечних об'єктів вимагає, в першу чергу, провести аналіз переходу повільного горіння у розвинену дефлаграцію і детонацію, виділивши таким чином проблему вибухобезпеки з більш загальної проблеми пожежної безпеки [1].

Нескінченно мале зміщення є полум'я вздовж осі О*х* є причиною збуреного стану всієї течії середовища (рис. 1).