МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДРОГОБИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ФРАНКА

Проблеми моделювання та розроблення інформаційних систем

Матеріали ІІІ науково-практичної інтернет-конференції

ДРОГОБИЧ, УКРАЇНА

1 червня 2018 року

є більше універсальним засобом і може успішно використовуватися для прийняття рішень і в інших сферах людської діяльності.

Список використаних джерел:

1. Lombardi L.A. A general business oriented language based on decision expression / L.A. Lombardi // Communications of the ACM. – 1964. – № 7 (2). – p. 104-111.

2. Humby E. Programs from decision tables / E. Humby. – London, Macdonald and Co.; New York, American Elsevier, 1973. – 91 p.

3. Karayev R.A., Sadikhova N.Y. Production-Tabular Knowledge Bases Tools for Assessing and Checking of Correctness/ R.A. Karayev // Middle-East Journal of Scientific Research. – 2014. – № 21 (9). – p. 1659-1662.

МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ МЕТОДУ ГЕНЕРУВАННЯ ПОТОКУ МАТРИЧНИХ КЛЮЧІВ ПЕРЕСТАНОВОК ТА ЇХ ЯКОСТІ

Красиленко В.Г., Нікітович Д.В.

Вінницький національний технічний університет

krasvg@i.ua

Переваги криптографічних перетворень (КП) текстографічних документів (ТГД) з візами, підписами, зображень (З), таблиць, діаграм, тощо, у криптосистемах матричного типу (МТ) [1-4] на основі алгоритмів і матрично-алгебраїчних моделей (МАМ), в тому числі узагальнених матричних афінних і афінно-перестановочних шифрів були продемонстровані у роботах [5-10]. Модифікації МАМ використовувались при створенні сліпих та інших цифрових підписів [11-14], вони дозволяють перевіряти у криптограмах чорно-білих, кольорових зображень наявність перекручувань, їх цілісність [5,7], створювати блокові [6], багатофункціональні параметричні моделі [8], багатосторінкові [9]

та досліджувати їх характеристики стійкості [10]. Базовими операціями МАМ є по-елементні множення, додавання за модулем матриць та матричні моделі перестановок (ММ_П) з процедурами множення матриць. Для реалізації КП необхідно матриці байтів зліва та справа множити на матриці перестановок (МП), матрицю з рядків, колонок, векторів, що в унітарних кодах відображають символи, коди, байти, теж замінювати, переставляти за допомогою перестановок. Для змін гістограми, збільшення ентропії криптограми З при їх КП на основі ММ_П необхідні декомпозиція R,G,B складових і їх бітових зрізів та декілька матричних ключів (МК) і векторних (ВК) [3-5]. Тобто для МАМ є гостра необхідність формування цілої низки МП з головного МК, які б задовольняли ряду вимог. Оскільки в [15,16] розглядались питання узгодження лиш головного МК загального виду, а не низки (потоку) МП, то **метою роботи** є моделювання та дослідження процесів формування потоку МП для МАМ КП у системах МТ, перевірка статистичних і кореляційних властивостей низки генерованих МП.

Розглянемо ситуацію, коли для КП блоків довжиною 256*256 байтів, що представлені у вигляді матриці чорно-білого зображення, чи векторів довжиною 256 байтів (2048 біт) використовуються МП розміром 256*256, описані в [2-5], де наведені процеси їх генерації, МАМ їх перетворень та КП на їх основі. Оскільки для кожного блоку, декількох раундових, циклових КП бажано мати низку МК, генерованих з головного ключа, наприклад, такої ж МП, то, з урахуванням вимог до крипто-статистичних характеристик МК, стає актуальною задача дослідження процесів швидкого надійного генерування послідовності МК у виді МП. Припустимо, що їх кількість теж дорівнює 256. Результати моделювання процесів генерування низки МП для такої ситуації у Mathcad з формулами та матрицями МП показані на рис. 1. Якщо головним МК є сформована випадкова МП KPX (рис. 1), то вона однозначно відображається 256-компонентною перестановкою (вектором) V_KPX та ще й у вигляді З чи

матриці байтів (МБ) розміром 16*16 з тією особливістю, що всі 256 її градацій інтенсивності є різними.

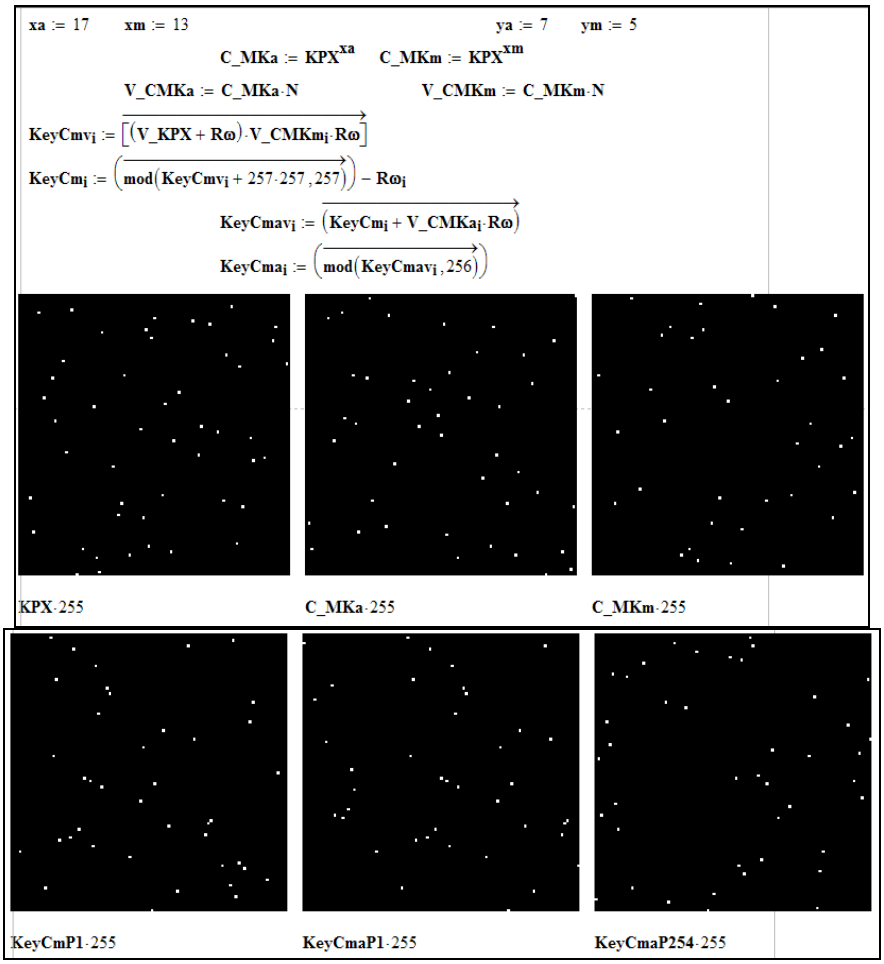


Рис. 1. Результати моделювання процесів генерування масиву МК (МП)

Використовуючи узгоджені сторонами скаляри *xa* та *xm*, як степені KPX сформуємо з KPX дві додаткові матриці C_MKa, C_MKm, дивись рис. 1, та відповідні їм вектори V_CMKa, V_CMKm, що разом з вектором V_KPX (векторне представлення KPX) показані на рис. 2. Гістограми всіх цих векторів (базових!) є горизонтальними лініями, дивись рис. 3, як і всіх векторних представлень генерованих перестановок, що утворюються з V_KPX, як його і-ті криптограми, за допомогою афінного шифру та пари і-их компонентів векторів V_CMKa, V_CMKm (адитивна і мультиплікативна складові). Ці криптограми і є і-ими поточними перестановками (векторами) KeyCma, що можуть однозначно

представлятись і у вигляді бітових матриць KeyCmaP розмірністю (256*256), наприклад, KeyCmaP1-254, рис.1. Фрагменти з вікон Mathcad показані на рис. 4.

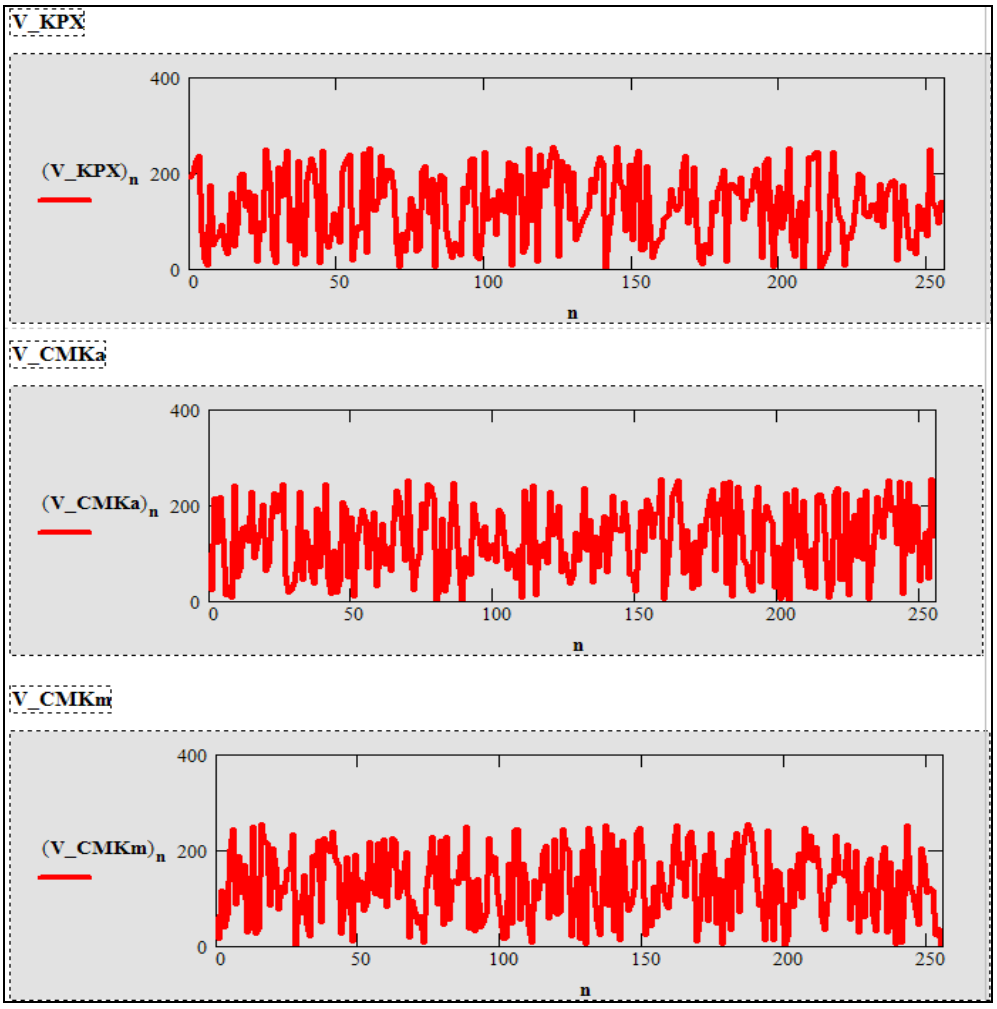


Рис. 2. Векторні представлення базових МК для генерування з них масиву МК (МП)

Оскільки гістограми всіх МП (їх векторів) є горизонтальними лініями, а їх ентропія рівна 8 біт, то крипто-аналіз на їх основі унеможливлюється. Крім того, головний та 2 допоміжні МК секретні, що дозволяє лише сторонам КП створювати чи мати цю низку МК (МП). В принципі, секретним чи узгодженим сторонами може бути лише головний та вищезгадані *xa* і *xm* скалярні ключі.

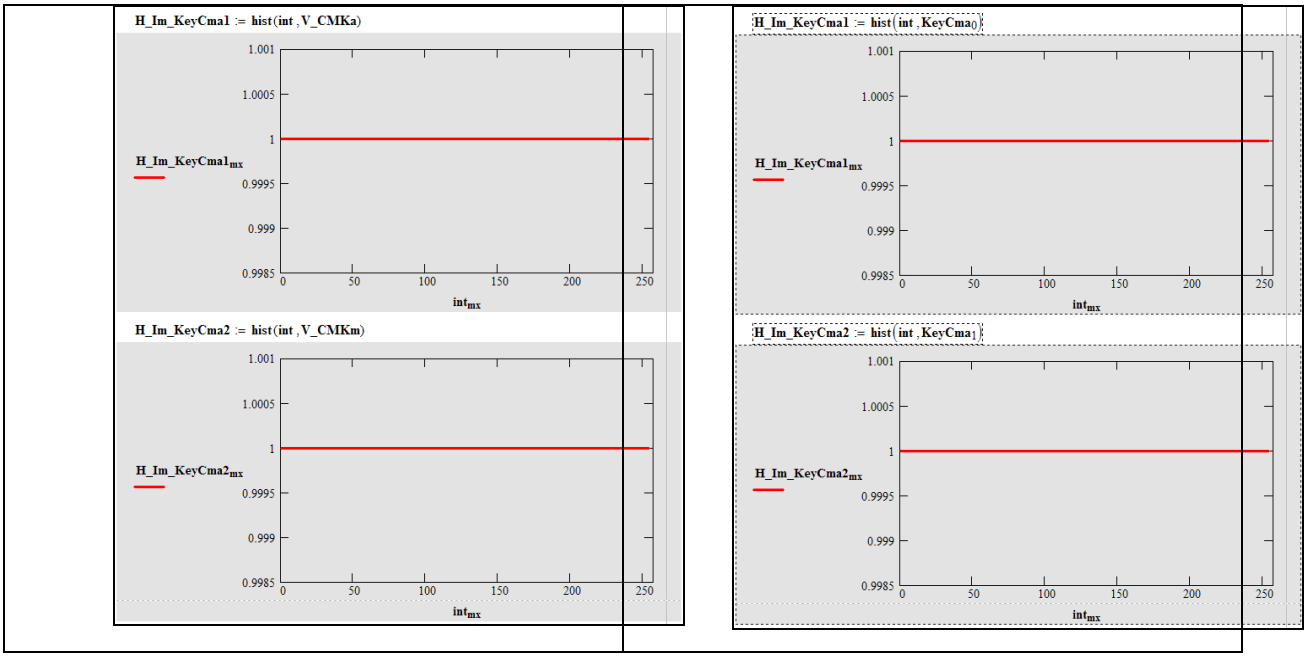
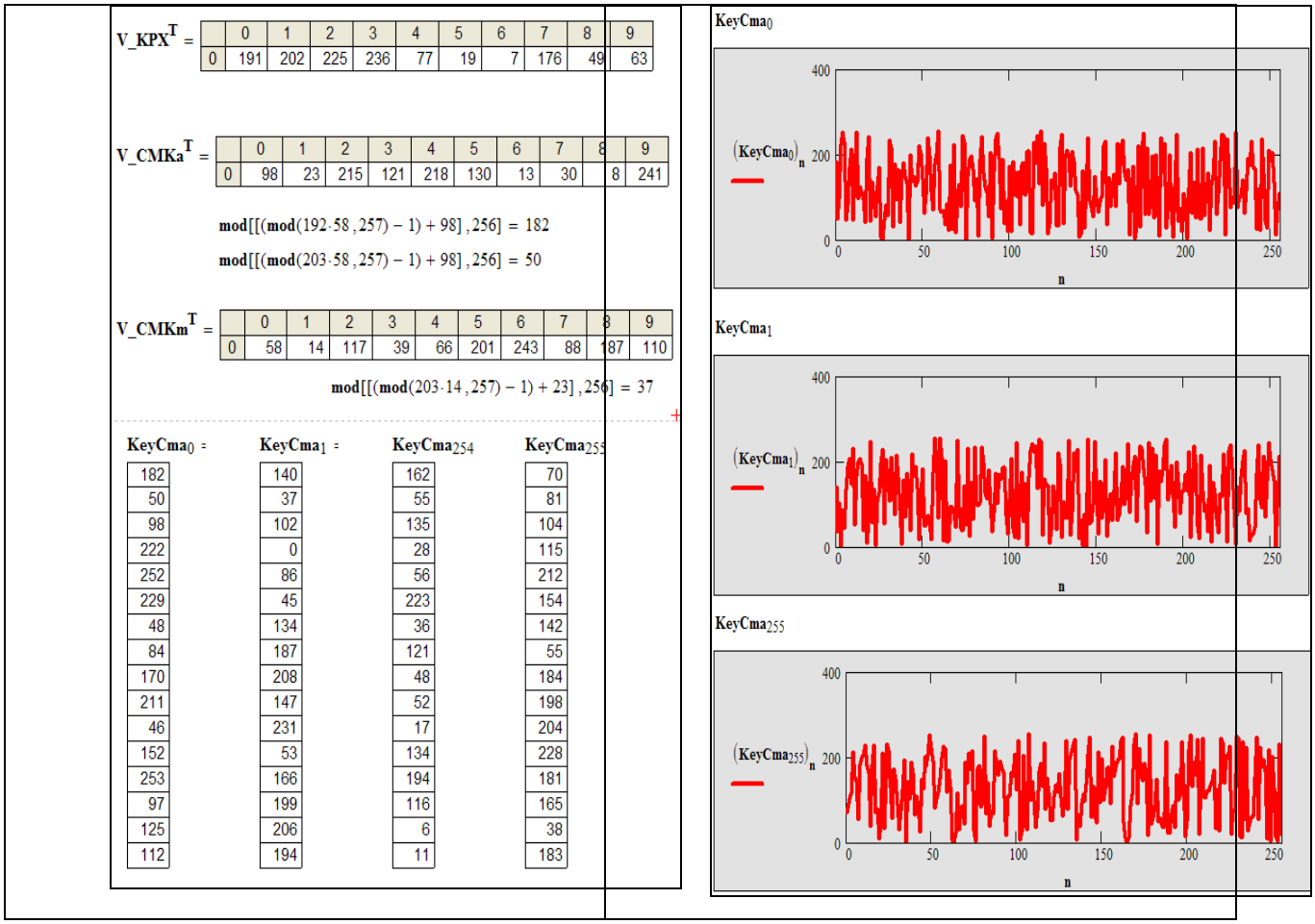


Рис. 3. Гістограми векторних представлень базових (ліворуч) та деяких (перший, другий) генерованих (праворуч) МК (МП)



V_KPX^T =

	0	1	2	3	4	5	6	7	8	9
0	191	202	225	236	77	19	7	176	49	63

V_CMKa^T =

	0	1	2	3	4	5	6	7	8	9
0	98	23	215	121	218	130	13	30	8	241

mod[[(mod(192·58 , 257) − 1) + 98] , 256] = 182

mod[[(mod(203·58 , 257) − 1) + 98] , 256] = 50

V_CMKm^T =

	0	1	2	3	4	5	6	7	8	9
0	58	14	117	39	66	201	243	88	187	110

mod[[(mod(203·14 , 257) − 1) + 23] , 256] = 37

KeyCma0 =	KeyCma1 =	KeyCma254	KeyCma255
182	140	162	70
50	37	55	81
98	102	135	104
222	0	28	115
252	86	56	212
229	45	223	154
48	134	36	142
84	187	121	55
170	208	48	184
211	147	52	198
46	231	17	204
152	53	134	228
253	166	194	181
97	199	116	165
125	206	6	38
112	194	11	183

Рис. 4. Фрагменти з вікон Mathcad: одна з процедур формування ключів (ліворуч) та векторні представлення деяких (нульовий, перший, 255-ий) генерованих (праворуч) МК (МП)

Для дослідження якості МК (МП) створеної низки, вивчення їх властивостей нами були розраховані всі їх можливі взаємно-кореляційні та еквівалентністні нормовані функції, що відображені у вигляді фрагментів вікон з Mathcad на рис. 5-7 та підтверджують досягнення напрочуд гарних властивостей. Зауважимо, що отримані результати та їх порівняння свідчать і про те, що взаємно-еквівалентністні нормовані функції є кращими за взаємно-кореляційні.

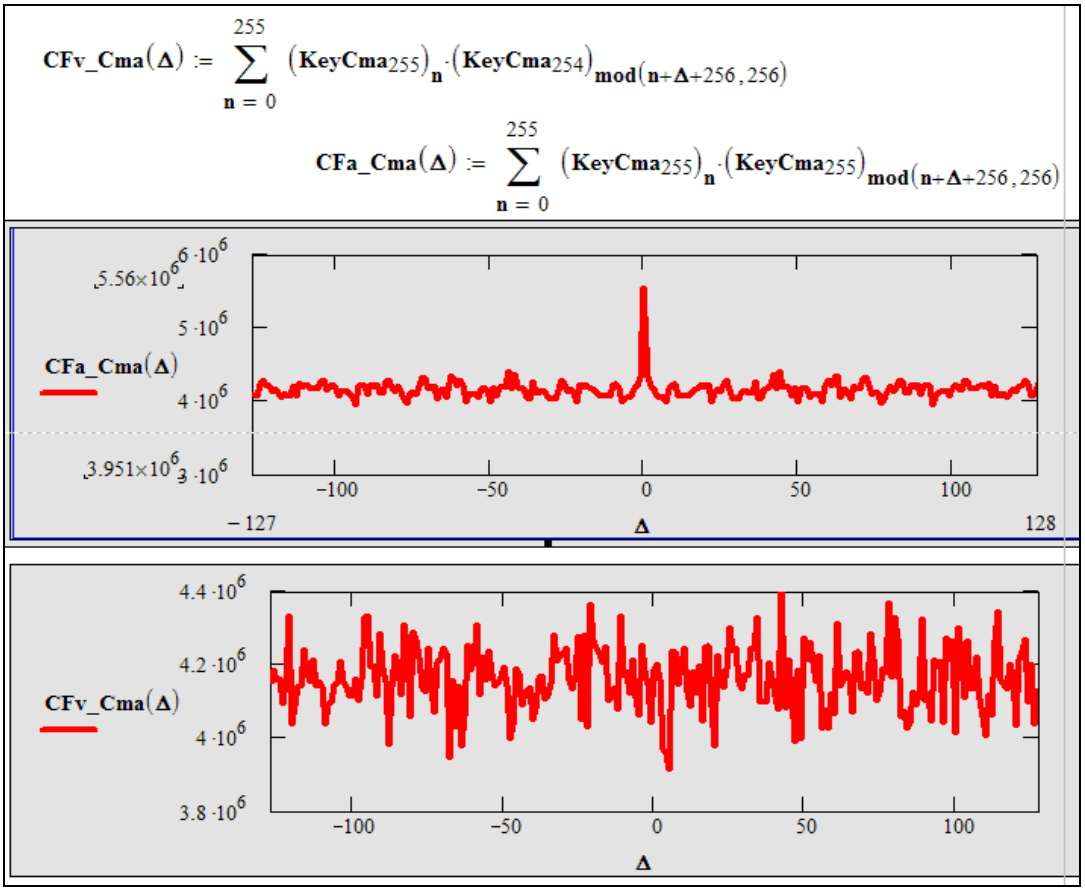


Рис. 5. Формули та вигляд авто-кореляційної CFa_Cma та взаємно-кореляційної CFv_Cma функцій в залежності від циклічного зсуву, зміщення елементів векторів МП

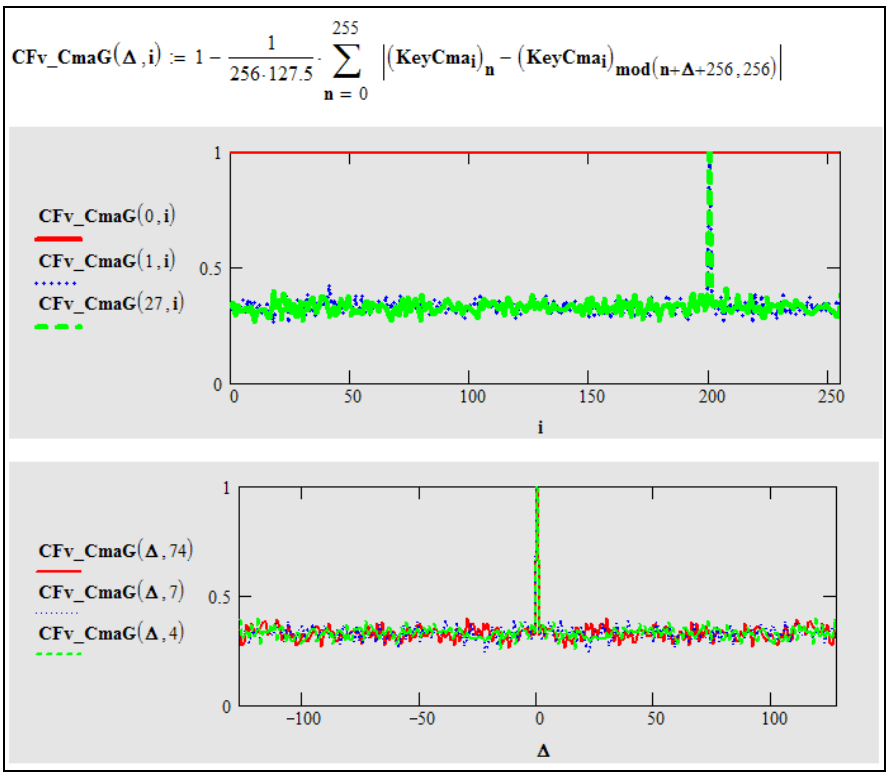


Рис. 6. Формули та вигляд взаємно-еквівалентністних CFv_CmaG функцій в залежності від номера МП (i) та циклічного зсуву, зміщення елементів векторів МП

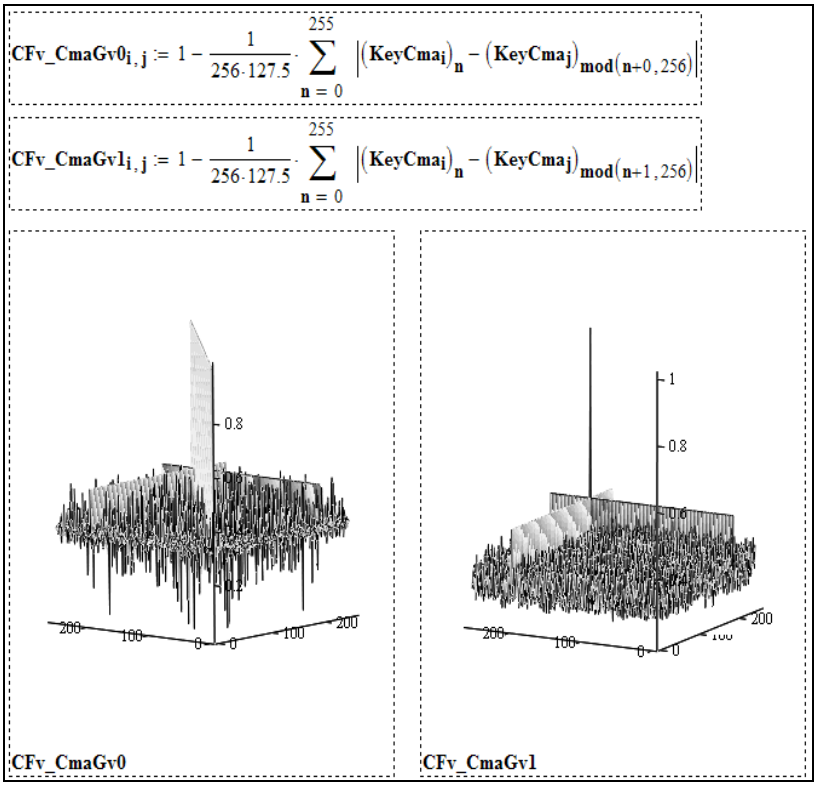


Рис. 7. Формули та вигляд (3D) взаємно-еквівалентністних CFv_CmaG функцій в залежності від номерів МП (i,j) для «0-го» і «1-го» зміщень елементів векторів МП

Для кращого сприйняття та більш ефективної передачі базових МК (МП) та послідовності створюваних МП останні за допомогою програмних модулів перетворюються у кольорові чи чорно-білі З, що показані на рис. 8 і можуть йти як фрейми відео-потоку (кольорове З відповідає трьом базовим МК).

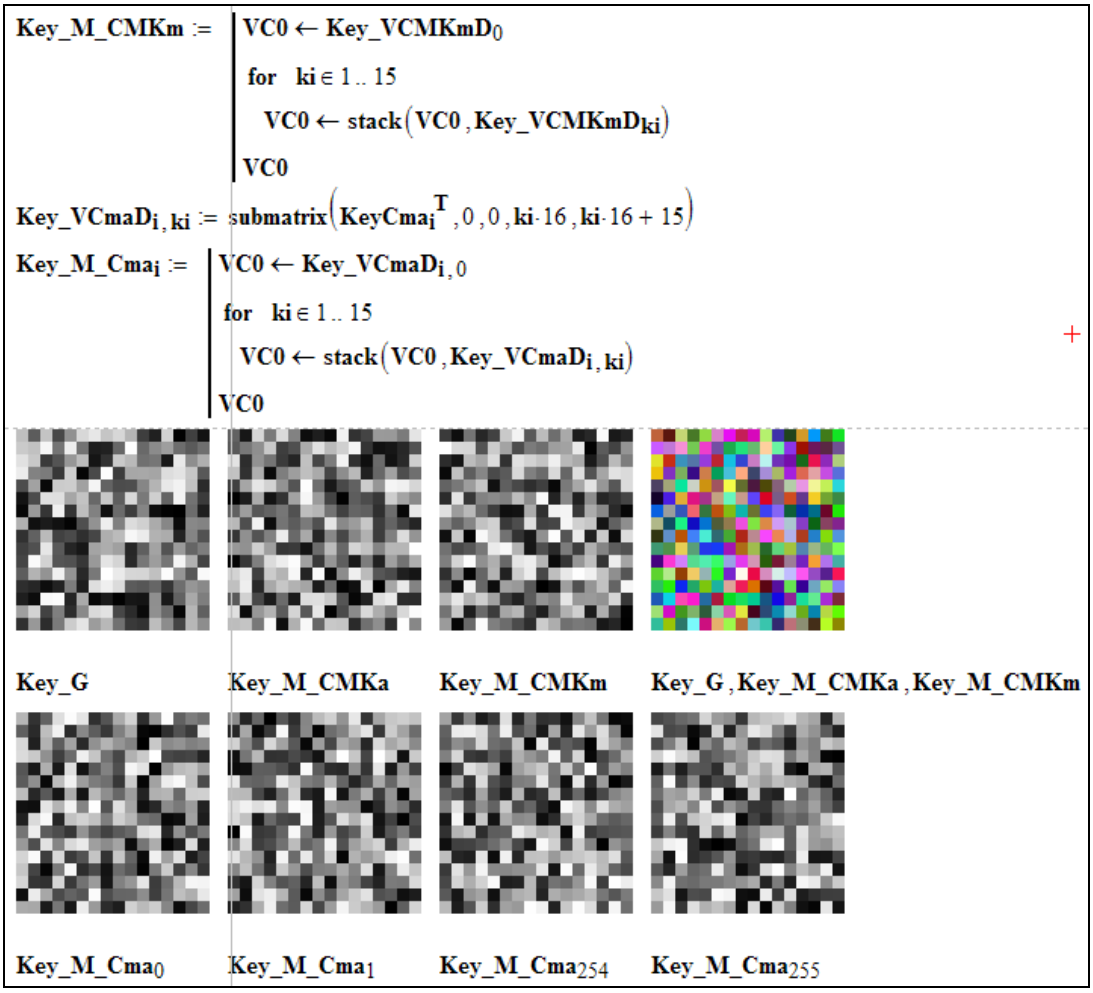


Рис. 8. Матричне представлення базових МК та низки МП

Як видно з рис.6-7, для одного МП (у експерименті 200-го) є схожість з іншим ключем, але це пояснюється тим, що для нього *xm* дорівнює «1». Це легко усувається, якщо кількість МП у послідовності зменшити з 256 до 255 для обраної при моделюванні та описаної тут ситуації.

Висновок. Запропонований і промодельований в Mathcad метод генерації низки МК (МП) для багатосторінкових, блокових, матричних афінно-перестановочних алгоритмів та МАМ КП. Досліджені властивості низки МК

(МП) за допомогою взаємно еквівалентністних нормованих функцій, що є ефективнішими за кореляційні, та підтверджено адекватність, стійкість методу.

Список використаних джерел:

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. НУ «Львів. Політехніка». – 2009. – № 658. – С. 59-63.

2. Красиленко В.Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2012. – Вип. 3(2). – С. 53-61. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15.

3. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельн. НУ. Технічні науки. – 2014. – № 1. – С. 74-79.

4. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т. – 2016. – № 23. – С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9.

5. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження /

В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.117-122.

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

8. Красиленко В.Г. Багатофункціональні параметричні матрично-алгебраїчні моделі (МАМ) криптографічних перетворень (КП) з операціями за модулем та їх моделювання. / В.Г. Красиленко, Д.В. Нікітович. // 72 НПК: матеріали конференції (13-15 грудня 2017 року). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.123-128.

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей ІІІ Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82. – Режим доступу: http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf

11. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60-63.

12. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей

матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. – С. 312 -318.

14. Красиленко В.Г. Моделювання покращених сліпих електронних цифрових підписів 2D типу / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп’ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної науково-технічної конференції, 20-21 квітня 2018 року. – Житомир: Вид. О.О. Євенок, 2018. – С. 78-82.

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

16. Красиленко В.Г. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів / В.Г. Красиленко, Д.В. Нікітович // Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/134/section/27 .

ЗМІСТ

Секція 1
Інтелектуальні інформаційні технології

Секція 2
Моделювання та дослідження складних систем

Секція 3
Інформаційні технології соціокомунікаційних систем та мереж

Секція 4
Інформаційно-комунікативні технології в освіті та наукових дослідженнях