International Science Group

ISG-KONF.COM

# IX

# INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE "THEORETICAL AND PRACTICAL ASPECTS OF THE DEVELOPMENT OF SCIENCE AND EDUCATION"

Prague, Czech Republic

March 05 - 08, 2024

ISBN 979-8-89292-739-0

DOI 10.46299/ISG.2024.1.9

# КООПЕРАТИВНИЙ ПРОТОКОЛ УЗГОДЖЕННЯ ВЕЛИКОРОЗМІРНИХ ІЗОМОРФНО ПРЕДСТАВЛЕНИХ СЕКРЕТНИХ КЛЮЧІВ-ПЕРЕСТАНОВОК ТА ЙОГО МОДЕЛЮВАННЯ

**Красиленко В. Г.,**
Кандидат технічних наук, доцент
Вінницький національний аграрний університет

**Нікітович Д. В.,**
Аспірант
Вінницький національний технічний університет

**Анотація:** Розглядаються процеси генерування матриць перестановок значної розмірності та їх матричних степенів, у тому числі в їх нових ізоморфних просторах, їх особливості та переваги для моделювання протоколу узгодження групою учасників головного кооперативного секретного ключа-перестановки. Запропоновано операції багатократних перестановок замість піднесення відповідних їм матриць перестановок у степені, що є базовими процедурами пропонованого кооперативного протоколу узгодження спільного секретного ключа-перестановки, який формується і передається у його ізоморфному представленні. Верифіковано запропоновані прискорені методи піднесення перестановок у значні степені. Наведені результати моделювання кооперативного протоколу узгодження секретного ключа-перестановки в цілому, його алгоритмічних кроків, операцій, що продемонстрували адекватність та переваги ізоморфних представлень для опису та процесів функціонування матричних моделей та запропонованого протоколу.

**Ключові слова***:* кооперативний протокол узгодження секретного ключа, матричні моделі**,** ізоморфні ключі-перестановки, криптограми, криптографічне перетворення.

**Вступ**. В епоху інформаційного суспільства та масових електронних комунікацій, широкого застосування інформаційних технологій (ІТ), постійного збільшення обсягів інформаційних потоків, їх значимості та необхідної стійкості до потенційних загроз важливе місце серед великої кількості різних технологій, методів та засобів захисту інформації займають криптографічні системи, які найбільш надійно здійснюють захист інформаційних об’єктів (ІО). За останні два-три десятиріччя суттєво зросла частка специфічних текстографічних документів (ТГД) у вигляді цифрових, табличних даних, малюнків, графіків, діаграм, підписів, віз, резолюцій, тощо, які є зображеннями значної розмірності і які необхідно передавати таємно. Багато з них містять інформацію з обмеженим чи закритим доступом, яку треба надавати як звітність у державні органи, засвідчувати їх цифровими підписами. Більшість використовуваних методів та

засобів криптографічних перетворень (КП) інформаційних масивів, зображень орієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати. Одним з ключових питань застосування криптографії, стеганографії є процеси (протоколи) узгодження електронним шляхом спільних секретних ключів чи низки похідних від них під-ключів. Проте, більшість протоколів, наприклад, Діффі-Хелмана, MTI, STS, тощо, як і більшість методів криптографічних перетворень (КП) ІО, зорієнтовані на суто скалярні ключі та послідовну обробку блоків. Навіть для симетричних, широко використовуваних, алгоритмів (на основі діючого стандарту AES, IDEA, тощо) типові довжини блоків та ключів складають 256-1024 бітів, хоч для деяких виняткових шифрів FEAL, RC6 та інших новітніх модифікацій широкого спектру відомих шифрів ці довжини обмежуються 1К-2К бітами [1]. Перехід від форматів даних скалярного типу у відомих системах до більш відповідних та природніх матрично-тензорних форматів інтенсифікував пошук нових матрично-алгебраїчних моделей (МАМ) криптографічних перетворень (КП) 2D (3D) - масивів, зображень (З). Темпи розвитку методів крипто-аналізу, обчислювальних засобів спонукають до збільшення довжин ключів (ДК), тому актуальним є пошук нових концепцій, що зорієнтовані на паралельні матричні процесори та моделі матричного типу (МТ). На основі МАМ появився новий клас криптосистем матричного типу (КМТ) [2-5]. Як відповідь на збільшення складності вирішуваних завдань та об’ємів інформації, яку до того ж все частіше необхідно переробляти в реальному часі, створення високопродуктивних паралельних матричних чи багатопроцесорних комп’ютерів та алгоритмів спричинило появу низки зорієнтованих на ці засоби модифікацій відомих алгоритмів КП та створення відповідних моделей матричного типу (МТ) [6-11]. Виявлені в цих роботах переваги таких криптосистем на основі МАМ, сприяли інтенсифікації досліджень МАМ та появі публікацій [6-10], у яких було продемонстровано цілу низку нових їх покращень та запропоновано розширення областей їх ефективного застосування.

**Аналіз останніх досліджень і публікацій**. Матричні афінні та афінно-перестановочні шифри (МАПШ) на основі нових просунутих МАМ, їх модифікації досліджувались та використовувались для криптографічних перетворень (КП) зображень, при створенні покращених електронних цифрових підписів [11-15], для маскування (приховування) зображень і відеофайлів [16-19], для генерування необхідних для цього потоків секретних матричних ключів різного типу [20-21]. Використання пропонованих матричного підходу та МАМ дозволило створювати блокові [7], параметричні [9], багатосторінкові [10] криптографічні моделі з їх підвищеною криптостійкістю [10] для 2D масивів, чорно-білих, кольорових зображень та перевіряти цілісність криптограм і наявність у них перекручувань [5, 6, 8]. Функціонування всіх таких МАМ підтверджено імітаційними моделюваннями, де показано переваги таких моделей, алгоритмів: розширені функціональні можливості, краще відображення при їх апаратних реалізаціях на матричні процесори. Вище перераховані факти свідчать про те, що традиційні процеси (протоколи) узгодження електронним шляхом спільних секретних ключів [22], чи низки похідних від них під-ключів,

слід адаптувати під новітні виклики [23-25], в тому числі і під криптосистеми МТ[24, 26, 27]. Практично для всіх відомих алгоритмів та шифрів, включно з новостворюваними [5-14], процедури переставляння бітів, байтів чи їх груп є найбільш поширеними та обов'язковими. Однією з основних складових узагальнених багатокрокових матричних афінно-перестановочних шифрів є матричні моделі перестановок (ММ_П) [3, 5, 6], які мають наочну простоту. Запропоновані в [27] модифіковані ММ_П з декомпозицією бітових зрізів усувають недоліки простих ММ_П, але потребують крім двох матричних ключів (МК) ще й двох векторних (ВК). Для реалізації всіх вищезгаданих матричних моделей (ММ) необхідні специфічні ключі у вигляді двовимірних масивів (зображень). Необхідність виконання КП над великорозмірними багатовимірними ІО, зображеннями (З) також потребує не лише матрично-алгебраїчних моделей (МАМ) КП, але і секретних матричних ключів (МК) [27, 28]. Подальші вдосконалення (ММ) КП з метою зашифрування багатовимірних сигналів, багато-спектральних зображень різних фізичних, аерокосмічних об'єктів потребує й однорідних до їх структури секретних матричних ключів, наприклад, у вигляді матриць (зображень) [28, 29]. Аналогічні МК потрібні і для розглянутих в [6] модифікованих ММ КП з верифікацією цілісності криптограм. Крім того, такі МК для таких ММ повинні враховувати специфіку та структуру форматів та розширень, які характерні для чорно-білих багато-градаційних, кольорових, багато-спектральних зображень.

**Постановка проблеми.** Стосовно МК 1-ого типу у вигляді випадкового (шумового) З, який був позначений нами як МК_З (від «зображення»), то нами ще в 2008р. було запропоновано узагальнення протоколу Діффі-Хелмана на матричний випадок і метод формування МК_З. Удосконаленню таких матричних протоколів за рахунок застосування покращених методів організації прискорених обчислень на основі паралельної матричної логіки присвячені роботи [26, 27], в яких були підтверджені модельними експериментами переваги багатокрокових, багатоступеневих протоколів узгодження секретного МК_З. Для МАПШ необхідно мати крім такого МК_З ще й матричні ключі 2-го типу, а саме, набір бінарних матриць перестановок [3, 6, 26, 27], позначимо тут їх як МК_П. Питання щодо їх формувань і застосувань частково розглядались в [3, 6, 26 ], і лише в [28] запропоновано протокол узгодження МК вже типу МК_П. Проте в ній не розглядались протоколи для випадків узгодження МК_П, що був би спільний для всіх учасників групи, тобто ситуації, коли учасники бажають створити свій кооперативний груповий МК_П. На відміну від протоколів з [26, 27], у [29] був розглянутий, так званий авторами, кооперативний протокол, але стосовно МК_З. Відомо з [6, 8], що генерація низки ПК типу МК_П, що створюються з головного ключа (ГМК_П зі збільшеною на порядки розмірністю), дозволяє успішно вирішувати проблему стійкості. А тому актуальною та важливою є задача узгодження секретного ГК типу МК_П значної розмірності, але саме кооперативного для учасників групи. Тому **метою роботи** є розробка, моделювання, дослідження криптографічного кооперативного протоколу узгодження спільного секретного МК_П для МАМ КП на основі

застосування нових ізоморфних представлень МК_П та аналізу процедур здійснення протоколу.

**Виклад основних результатів.** Для вибраного нами 1-го експерименту МК_П була бітовою квадратною матрицею (PSAB) розміром 256*256 ел. Моделювання протоколу для випадку піднесення МК_П у випадкові, відомі лише сторонам (двом для ясності) обміну, степені, показано на рис.1. Навіть знання МК_П – основи при значній потужності множини перестановок (N!=256!), де N - розмірність МК_П) не дає можливості без перехоплення обох створених сторонами МК_П взнати ключ.

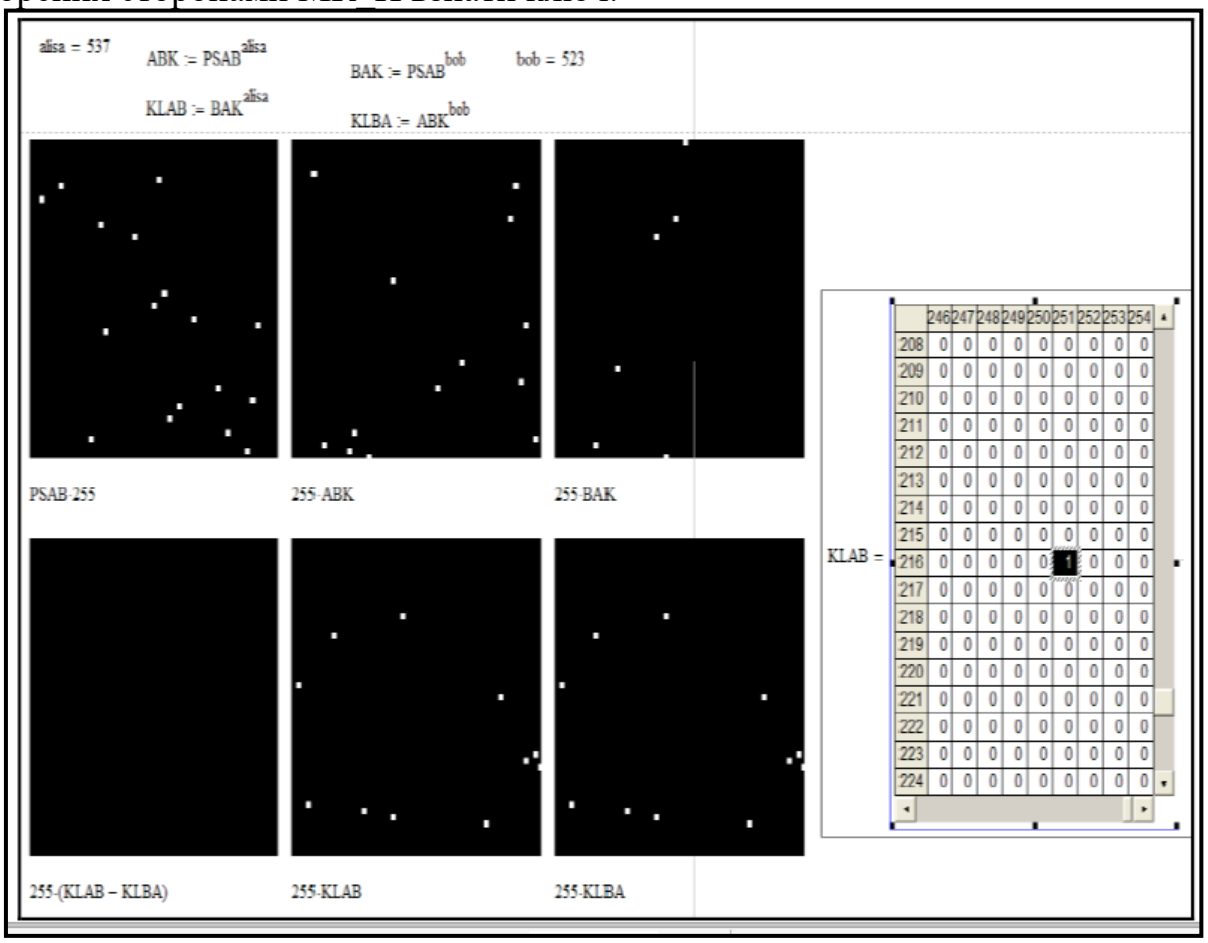



Рис. 1 Фрагмент вікна Mathcad з верифікацією модифікації протоколу Діффі-Хелмана для випадку піднесення у степені (537 та 523) МК_П, як основи. Вигляд основи (матриця PSAB 256*256), проміжних МК_П (ABK, BAK), що ними обмінюються сторони, та утворених ключів (KLAB, KLBA), які однакові

Для 2-го експерименту в якості МК_П було взято бітову квадратну матрицю з N*N елементами («0» чи «1»), де $N=2^{\wedge 16}$, що збільшило потужність множини перестановок до значення (65536 !). Таким чином, довільну перестановку довжиною 65536 (бітову матрицю 65536*65536 ел.) можна однозначно ізоморфно відобразити двома матрицями розміром 256*256, елементи яких приймають значення з діапазону 0-255. Вікно Mathcad з модулем для генерування базового (головного) МК (ГМК_П) та виглядом його складових KeyA та KeyB (двох напівтонових зображень) показано на рис.2. Програмний

модуль (копії з Mathcad), який реалізує процедуру ітераційних перестановок в МК_П, ізоморфних піднесенню матриці перестановки у потрібну степінь, показано на рис.3. Подібні йому використовувались для всіх покрокових процедур при імітаційному моделюванні кооперативного протоколу.


Рис. 2. Програмний модуль для генерування базового (головного) МК_П та вигляд його двох складових KeyA та KeyB у форматі двох чорно-білих зображень (Вікно Mathcad).

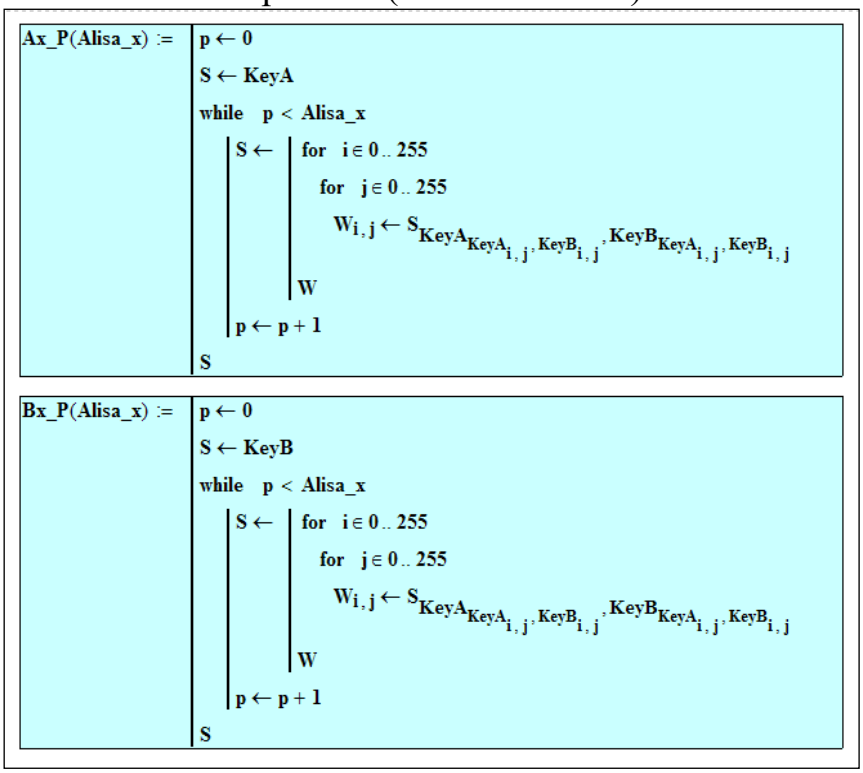



Рис. 3. Програмні модулі (копії з Mathcad), що відображають процедуру ітераційних перестановок в МП, ізоморфних піднесенню матриці перестановки у потрібну степінь стороною *x* (Alisa)

Піднесення матриць-перестановок МК_П (N*N бінарних, де $N=2^{16}$) еквівалентно замінюється швидкими перестановками, які додатково можуть бути ще більш прискореними при значних степенях за рахунок використання деякого базового набору фіксованих (фіксовані степені ГМП) та специфічної їх послідовності. Моделюванням нами було перевірено адекватність прискорених

алгоритмів ізоморфного формування степенів матричних перестановок. Для цього піднесені у матричну степінь бітові матриці після переведення їх у ізоморфний вигляд порівнювалися з матрицями, отриманими швидкими перестановками. Результати моделювання кооперативного протоколу для випадку трьох сторін показані на рис. 4-6. Протокол виконується так.

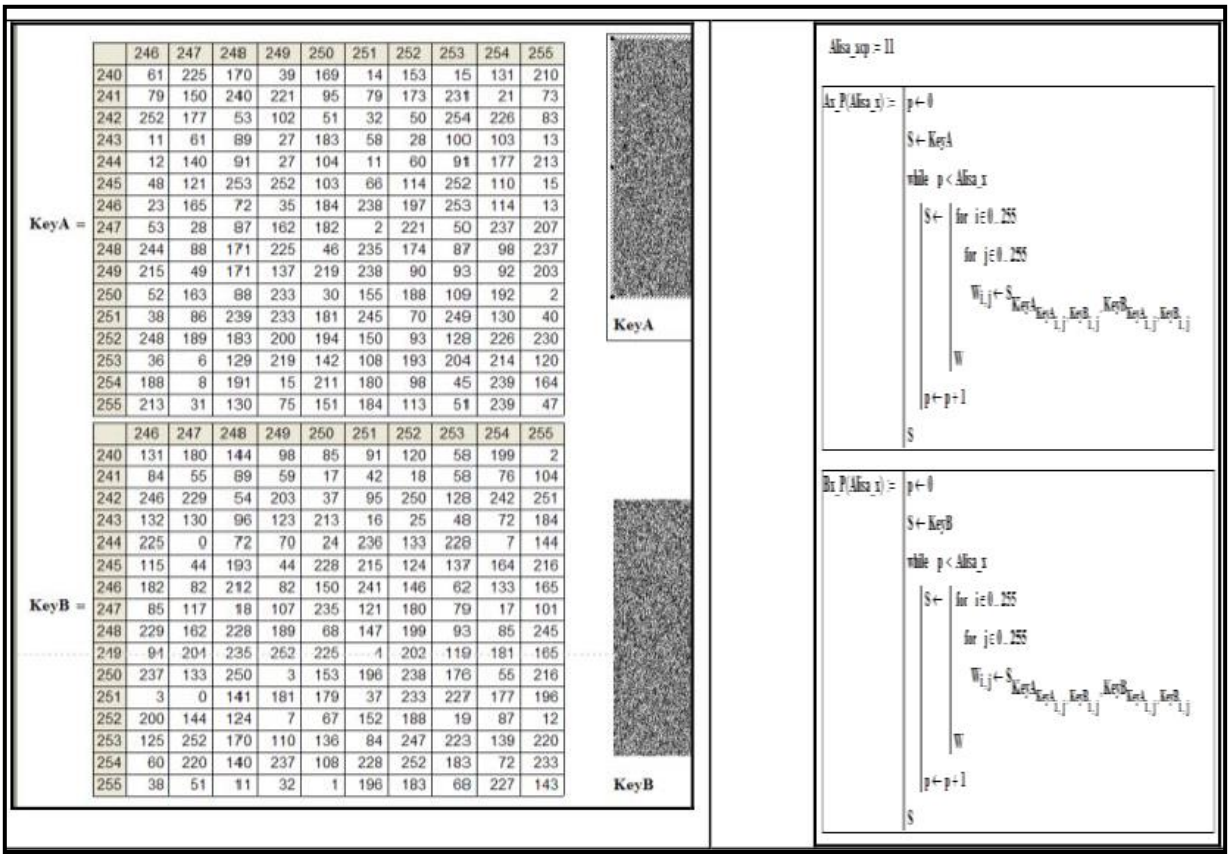



Рис. 4. Вікно Mathcad з вибраним великорозмірним МК_П, ізоморфно представленим двома складовими (KeyA, KeyB) у цифровому та візуальному виглядах, (ліворуч) та програмним модулем для багаторазових перестановок (праворуч).

Кожна з сторін x, y, z (Alisa, Bob, David) вибирають за основу спільну МК_П, ізоморфно представлену її складовими (KeyA, KeyB) та шлях послідовних передач між собою утворених на кожному кроці ними проміжних МК_П, що утворюються як степені основи в залежності від вибраних таємних ідентифікаторів-чисел: Alisa_x, Bob_y, David_z за допомогою програмних модулів перестановок, описаних та показаних на рис.3-4. Кожна з сторін на першому кроці підносить ізоморфно ГМК_П у вибрану ними свою секретну степінь, яка зазвичай на практиці є досить великим псевдовипадковим числом порядку типових величин, що застосовуються сьогодні в криптографії для суттєвого збільшення складності обчислень при перебірних атаках на односторонні функції. Після цього кожна сторона пересилає нову МК_П іншій стороні по вибраному шляху передач. Потім на наступних кроках сторони, отримані ними нові МК_П аналогічно підносять у ті ж свої випадкові секретні степені та отримані перестановки (зображення) знову передають по шляху.

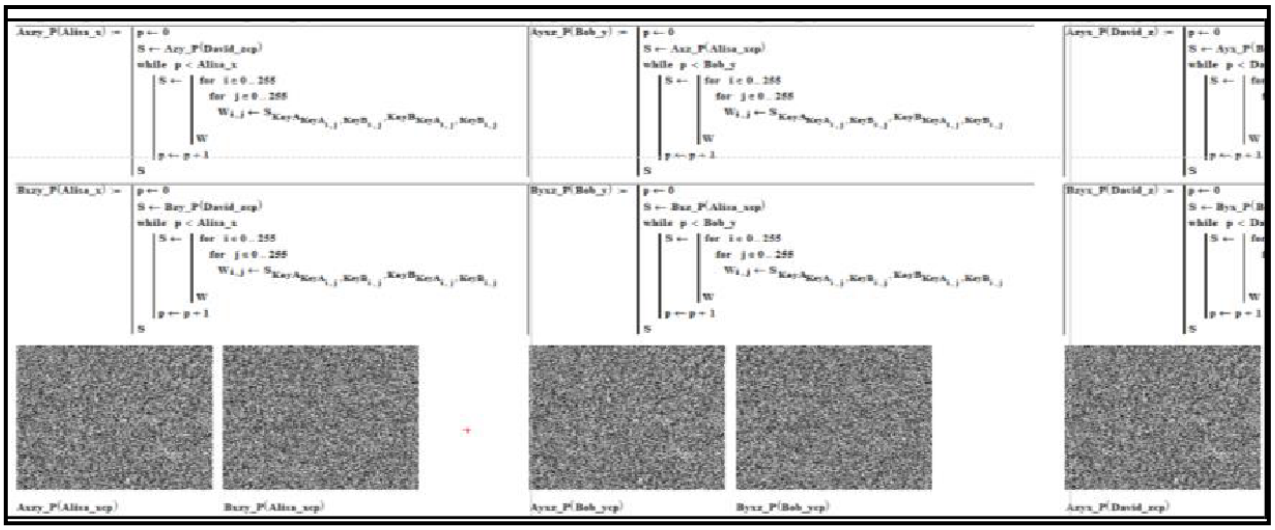
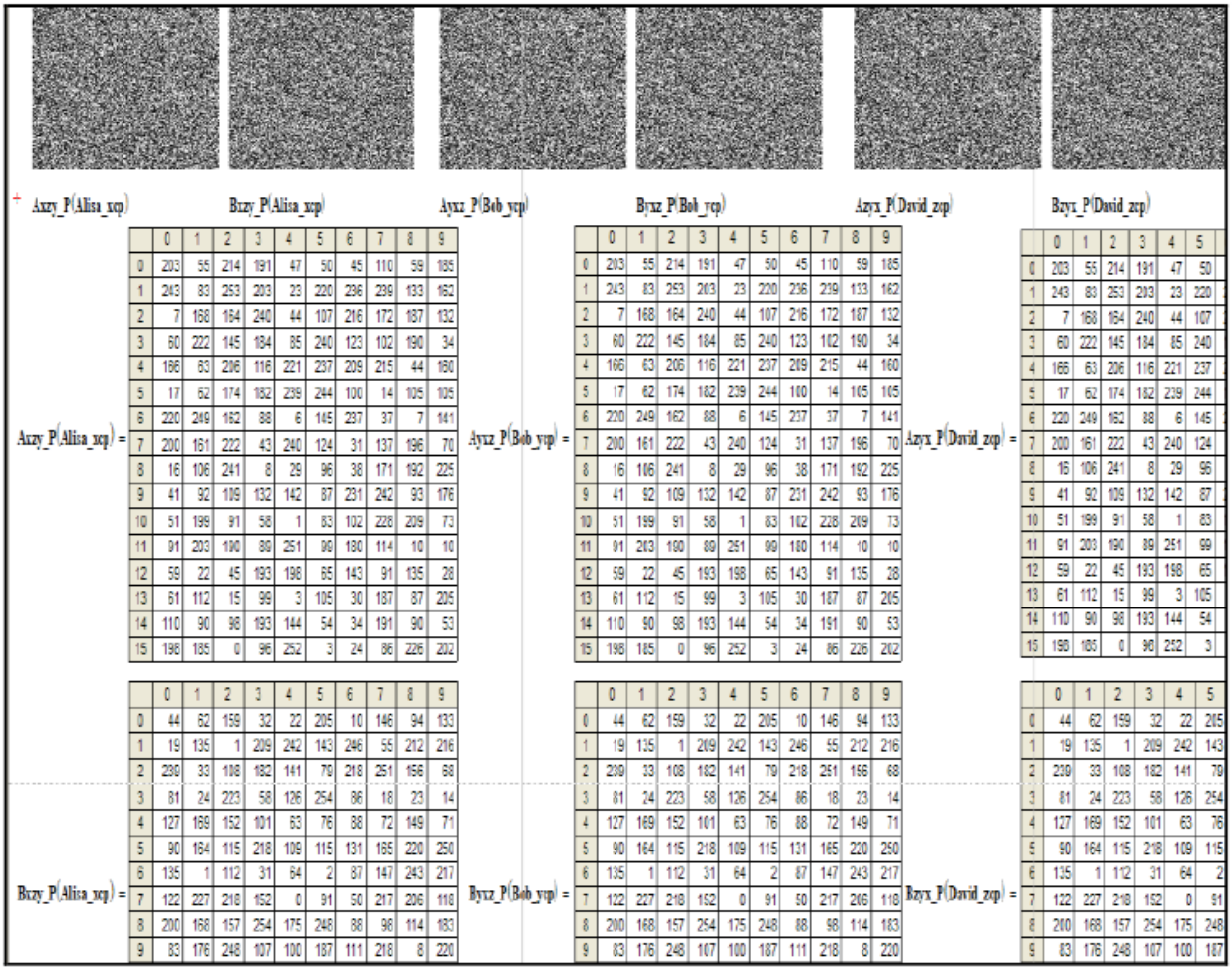


Рис. 5. Фрагменти вікна Mathcad для моделювання процесів утворення секретного МК_П трьома сторонами ( Alisa, Bob, David): модулі для перестановок, вигляд ключів



Axzy_P(Alisa_xcp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 203 | 55 | 214 | 191 | 47 | 50 | 45 | 110 | 59 | 165 |
| 1 | 243 | 83 | 253 | 203 | 23 | 220 | 236 | 239 | 133 | 162 |
| 2 | 7 | 168 | 164 | 240 | 44 | 107 | 216 | 172 | 187 | 132 |
| 3 | 60 | 222 | 145 | 184 | 85 | 240 | 123 | 102 | 190 | 34 |
| 4 | 166 | 63 | 206 | 116 | 221 | 237 | 209 | 215 | 44 | 160 |
| 5 | 17 | 62 | 174 | 182 | 239 | 244 | 100 | 14 | 105 | 105 |
| 6 | 220 | 249 | 162 | 88 | 6 | 145 | 237 | 37 | 7 | 141 |
| 7 | 200 | 161 | 222 | 43 | 240 | 124 | 31 | 137 | 196 | 70 |
| 8 | 16 | 106 | 241 | 8 | 29 | 96 | 38 | 171 | 192 | 225 |
| 9 | 41 | 92 | 109 | 132 | 142 | 87 | 231 | 242 | 93 | 176 |
| 10 | 51 | 199 | 91 | 58 | 1 | 83 | 102 | 228 | 209 | 73 |
| 11 | 91 | 203 | 190 | 89 | 251 | 99 | 180 | 114 | 10 | 10 |
| 12 | 59 | 22 | 45 | 193 | 198 | 65 | 143 | 91 | 135 | 28 |
| 13 | 61 | 112 | 15 | 99 | 3 | 105 | 30 | 187 | 87 | 205 |
| 14 | 110 | 90 | 98 | 193 | 144 | 54 | 34 | 191 | 90 | 53 |
| 15 | 198 | 185 | 0 | 96 | 252 | 3 | 24 | 86 | 226 | 202 |

Bxzy_P(Alisa_xcp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 44 | 62 | 159 | 32 | 22 | 205 | 10 | 146 | 94 | 133 |
| 1 | 19 | 135 | 1 | 209 | 242 | 143 | 246 | 55 | 212 | 216 |
| 2 | 239 | 33 | 108 | 182 | 141 | 79 | 218 | 251 | 166 | 68 |
| 3 | 81 | 24 | 223 | 58 | 126 | 254 | 86 | 18 | 23 | 14 |
| 4 | 127 | 169 | 152 | 101 | 63 | 76 | 88 | 72 | 149 | 71 |
| 5 | 90 | 164 | 115 | 218 | 109 | 115 | 131 | 165 | 220 | 250 |
| 6 | 135 | 1 | 112 | 31 | 64 | 2 | 87 | 147 | 243 | 217 |
| 7 | 122 | 227 | 216 | 152 | 0 | 91 | 50 | 217 | 206 | 118 |
| 8 | 200 | 168 | 157 | 254 | 175 | 248 | 88 | 98 | 114 | 183 |
| 9 | 83 | 176 | 248 | 107 | 100 | 187 | 111 | 218 | 8 | 220 |

Ayxz_P(Bob_ycp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 203 | 55 | 214 | 191 | 47 | 50 | 45 | 110 | 59 | 165 |
| 1 | 243 | 83 | 253 | 203 | 23 | 220 | 236 | 239 | 133 | 162 |
| 2 | 7 | 168 | 164 | 240 | 44 | 107 | 216 | 172 | 187 | 132 |
| 3 | 60 | 222 | 145 | 184 | 85 | 240 | 123 | 102 | 190 | 34 |
| 4 | 166 | 63 | 206 | 116 | 221 | 237 | 209 | 215 | 44 | 160 |
| 5 | 17 | 62 | 174 | 182 | 239 | 244 | 100 | 14 | 105 | 105 |
| 6 | 220 | 249 | 162 | 88 | 6 | 145 | 237 | 37 | 7 | 141 |
| 7 | 200 | 161 | 222 | 43 | 240 | 124 | 31 | 137 | 196 | 70 |
| 8 | 16 | 106 | 241 | 8 | 29 | 96 | 38 | 171 | 192 | 225 |
| 9 | 41 | 92 | 109 | 132 | 142 | 87 | 231 | 242 | 93 | 176 |
| 10 | 51 | 199 | 91 | 58 | 1 | 83 | 102 | 228 | 209 | 73 |
| 11 | 91 | 203 | 190 | 89 | 251 | 99 | 180 | 114 | 10 | 10 |
| 12 | 59 | 22 | 45 | 193 | 198 | 65 | 143 | 91 | 135 | 28 |
| 13 | 61 | 112 | 15 | 99 | 3 | 105 | 30 | 187 | 87 | 205 |
| 14 | 110 | 90 | 98 | 193 | 144 | 54 | 34 | 191 | 90 | 53 |
| 15 | 198 | 185 | 0 | 96 | 252 | 3 | 24 | 86 | 226 | 202 |

Byxz_P(Bob_ycp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 44 | 62 | 159 | 32 | 22 | 205 | 10 | 146 | 94 | 133 |
| 1 | 19 | 135 | 1 | 209 | 242 | 143 | 246 | 55 | 212 | 216 |
| 2 | 239 | 33 | 108 | 182 | 141 | 79 | 218 | 251 | 166 | 68 |
| 3 | 81 | 24 | 223 | 58 | 126 | 254 | 86 | 18 | 23 | 14 |
| 4 | 127 | 169 | 152 | 101 | 63 | 76 | 88 | 72 | 149 | 71 |
| 5 | 90 | 164 | 115 | 218 | 109 | 115 | 131 | 165 | 220 | 250 |
| 6 | 135 | 1 | 112 | 31 | 64 | 2 | 87 | 147 | 243 | 217 |
| 7 | 122 | 227 | 216 | 152 | 0 | 91 | 50 | 217 | 206 | 118 |
| 8 | 200 | 168 | 157 | 254 | 175 | 248 | 88 | 98 | 114 | 183 |
| 9 | 83 | 176 | 248 | 107 | 100 | 187 | 111 | 218 | 8 | 220 |

Azyx_P(David_zcp)

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 203 | 55 | 214 | 191 | 47 | 50 | 45 | 110 | 59 | 165 |
| 1 | 243 | 83 | 253 | 203 | 23 | 220 | 236 | 239 | 133 | 162 |
| 2 | 7 | 168 | 164 | 240 | 44 | 107 | 216 | 172 | 187 | 132 |
| 3 | 60 | 222 | 145 | 184 | 85 | 240 | 123 | 102 | 190 | 34 |
| 4 | 166 | 63 | 206 | 116 | 221 | 237 | 209 | 215 | 44 | 160 |
| 5 | 17 | 62 | 174 | 182 | 239 | 244 | 100 | 14 | 105 | 105 |
| 6 | 220 | 249 | 162 | 88 | 6 | 145 | 237 | 37 | 7 | 141 |
| 7 | 200 | 161 | 222 | 43 | 240 | 124 | 31 | 137 | 196 | 70 |
| 8 | 16 | 106 | 241 | 8 | 29 | 96 | 38 | 171 | 192 | 225 |
| 9 | 41 | 92 | 109 | 132 | 142 | 87 | 231 | 242 | 93 | 176 |
| 10 | 51 | 199 | 91 | 58 | 1 | 83 | 102 | 228 | 209 | 73 |
| 11 | 91 | 203 | 190 | 89 | 251 | 99 | 180 | 114 | 10 | 10 |
| 12 | 59 | 22 | 45 | 193 | 198 | 65 | 143 | 91 | 135 | 28 |
| 13 | 61 | 112 | 15 | 99 | 3 | 105 | 30 | 187 | 87 | 205 |
| 14 | 110 | 90 | 98 | 193 | 144 | 54 | 34 | 191 | 90 | 53 |
| 15 | 198 | 185 | 0 | 96 | 252 | 3 | 24 | 86 | 226 | 202 |

Bzyx_P(David_zcp)

| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 44 | 62 | 159 | 32 | 22 | 205 |
| 1 | 19 | 135 | 1 | 209 | 242 | 143 |
| 2 | 239 | 33 | 108 | 182 | 141 | 79 |
| 3 | 81 | 24 | 223 | 58 | 126 | 254 |
| 4 | 127 | 169 | 152 | 101 | 63 | 76 |
| 5 | 90 | 164 | 115 | 218 | 109 | 115 |
| 6 | 135 | 1 | 112 | 31 | 64 | 2 |
| 7 | 122 | 227 | 216 | 152 | 0 | 91 |
| 8 | 200 | 168 | 157 | 254 | 175 | 248 |
| 9 | 83 | 176 | 248 | 107 | 100 | 187 |

Рис. 6. Копія вікна Mathcad з утвореними трьома сторонами рівними секретними ключами МК_П у вигляді їх ізоморфних двох складових

Утворені МК_П (дві матриці по 256*256 байтів сторони передають сусідам по шляху, а потім підносять отримані МК знову у свої степені, дивись рис.5-6.

Усі протокольні дії виконуються з МК_П ізоморфного виду, а не зі скалярами. Сторони не знають ідентифікаторів (степенів) інших сторін, але отриманий ними секретний МК_П (ізоморфно у вигляді двох зображень) ключ для всіх учасників групи є однаковим. Отже результатом протоколу є тотожні ключі, таємний МК_П, рівність якого очевидна (рис.6) та забезпечена для всіх n сторін без знання їх ідентифікаторів.

Правильність функціонування протоколу підтверджена результатами моделювання у Mathcad. Аналіз стійкості, з урахуванням потужності множини утворюваних цим протоколом відповідних великорозмірних МК_П, показав неможливість здійснення атак, так як вже для $N=2^{16}$ ця потужність оцінюється величиною $(2^{16})!$.

**Висновки.** Виконано моделювання протоколу узгодження кооперативного секретного великорозмірного ключа-перестановки та підтверджено правильну його роботу, адекватність алгоритмічних кроків і методів формування проміжних, кінцевої МК_П. Перевірені алгоритми прискорених піднесень у значні степені матриць перестановок зі збереженням їх ізоморфних представлень, показані їх переваги.

## Список літератури

1. S. Zeadallya, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," Internet of Things, 2019, doi: 10.1016/j.iot.2019.100075. Elsevier.

2. Красиленко В.Г., Флавицька Ю.А. Моделювання матричних алгоритмів криптографічного захисту. Вісник НУ «Львів. політехніка». – 2009. – № 658. – С. 59-63.

3. Красиленко В. Г., Грабовляк С.К. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень. Системи обробки інформації. – 2012. – Вип. 3(2). – С. 53-61.

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

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

6. Красиленко В.Г., Нікітович Д.В. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітово-зрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності. Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127.

7. Красиленко В.Г., Нікітович Д.В. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження.- 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім., 2017. – Ч. 1. – С.117-122.

8. Красиленко В.Г., Нікітович Д.В. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями, Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2016. – № 23. – С. 31-36.

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

10. Красиленко В.Г., Нікітович Д.В. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок. «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.

11. Красиленко В.Г., Грабовляк С.К. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи.-Системи обробки інформації. –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., Нікітович Д.В. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів. Матеріали VI МНПК «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 МНПК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 78-82.

15. Красиленко В.Г. Моделювання покращених багатокрокових 2D RSA алгоритмів для криптографічних перетворень та сліпого електронного цифрового підпису / В.Г. Красиленко, Д.В. Нікітович, Р.О. Яцковська, В.І. Яцковський // Системи обробки інформації: збірник наукових праць, 2019. – Вип. 1 (156). – С. 92-100.

16. Vostrikov A., Sergeev M. Expansion of the Quasi-Orthogonal Basis to Mask Images // Intelligent Interactive Multimedia Systems and Services. Smart Innovations, Systems and Technologies 40. Springer, 2015. Pp. 161 – 168. DOI 10.1007/978-3-319-19830-9_15

17. 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.

18. Krasilenko V. G., Kychak V. M., Nikolskyy A. I., Lazarev A. A., Nikitovych D. V. Simulation of algorithms for detection, localization and tracking of moving

objects in video streams. Матеріали IX конференції «Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем (СПІРН-2023)», Вінниця, 15-17 листопада 2023 р. Вінниця, 2023. URL: https://conferences.vntu.edu.ua/index.php/spirn/spirn2023/paper/download/19349/16036 .

19. V.G. Krasilenko, A.A Lazarev, D.V Nikitovich, "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, pp. 170-214, 2020.

20. Krasilenko V. G. Podlubnyi V. F., Nikitovych D. V. Modeling a method for generating a stream of secret keys in the form of permutation matrices for encryption-masking of video frames and studying its characteristics. 2nd International Conference on Innovative Solutions in Software Engineering, 29-30 November 2023. Ivano-Frankivsk, 2023. Pp. 222-231. URL: https://doi.org/10.5281/zenodo.10397356

21. Красиленко В.Г., Нікітович Д.В. Моделювання процесів генерування матричних ключів.-«Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2018): Збірник тез доповідей IV МНПК, 17-18 травня 2018 року. – Черкаси: ЧДТУ, 2018. – С. 32-35.

22. W. Diffie, and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT22, No. 6, Vol. 22, No. 6, pp. 644-654, 1976.

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

24. Білецький А.Я., Білецький А.А., Кандиба Р.Ю. Матричні аналоги протоколу Діффі-Хеллмана. Автоматика, вимірювання та керування: Вісник нац. ун-ту "Львівська політехніка". – 2012. – № 741. – С. 128-133.

25. 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.

26. 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.

27. 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.

28. Красиленко В.Г., Нікітович Д.В. Протоколи узгодження секретних ключів у вигляді матричних перестановок значної розмірності для криптографічних перетворень. - Тези доповідей XI МНТК «ІКТ – 2020», м. Житомир, 9-11 квітня 2020 р., 2020. – С. 39-49.

29. Красиленко В.Г., Нікітович Д.В. Кооперативний протокол узгодження спільного секретного матричного ключа. - Матеріали VII МНПК (ІУСТ), 17 – 18 вересня 2018 р., Одеса. ОНПУ; ред. кол: В.В. Вичужанін. – Одеса, 2018. – С. 122–127.