https://doi.org/10.31649/1997-9266-2025-182-5-113-120

УДК 004.056.5

В. А. Лужецький[1]
М. С. Ціхоцький[1]

РОЗПОДІЛ СЕКРЕТНОГО ВМІСТУ ДАНИХ ЗА (*k, n*)-СХЕМОЮ З ВИКОРИСТАННЯМ ЗАШИФРОВАНИХ БЛОКІВ

[1]Вінницький національний технічний університет

Запропоновано порогову схему розподілу секретного вмісту даних великого обсягу, які попередньо зашифровано. Актуальність дослідження зумовлена постійним зростанням обсягів інформації, яка обробляється в сучасних інформаційних системах, що висуває додаткові вимоги до наявних схем розподілу секрету. Відомі схеми розподілу секрету, незважаючи на їх теоретичну обґрунтованість та доведену інформаційну безпеку, вимагають значних обчислювальних витрат, оскільки використовують складні математичні операції, та адаптовані для роботи з секретними даними невеликого обсягу (секретними ключами). Через це вони малопридатні для захисту даних великого обсягу. До того ж обсяг розподілених даних може значно перевищувати обсяг початкових даних.

Метою роботи є зменшення обсягу розподілених даних шляхом розробки (k,n)-схеми, що передбачає використання блоків попередньо зашифрованих початкових даних.

Особливість запропонованої авторами (k, n)-схеми розподілу секрету полягає в тому, що попередньо реалізується зашифрування секретних даних з подальшим їх розбиттям на n блоків та формування часток для учасників коаліції. Всі ці дії виконує дилер, який також відновлює секрет з часток, що надають йому учасники коаліції. Для відновлення даних необхідна наявність щонайменше k часток, а будь-яка коаліція, менша за порогове значення, не забезпечує можливість відновити секрет дилером. Дилер має свою власну частку, яка забезпечує можливість відновлення секрету, навіть якщо коаліція надає лише (n – 1) блоків.

У відомих схемах розподілу секрету сумарний обсяг розподілених даних в n разів більший за обсяг секрету. Проведені дослідження підтвердили, що запропонована авторами (k, n)-схема розподілу секрету забезпечує зменшення сумарного обсягу даних, які зберігають учасники коаліції. Коефіцієнт зменшення δ залежить від параметрів k і n та зростає зі збільшенням значення k.

Запропонована схема розподілу секрету має лінійну залежність складності реалізації від розміру вхідних даних, що є важливою перевагою у практичному застосуванні. Порівняно з відомими груповими схемами розподілу секрету забезпечується вища продуктивність. Підвищення продуктивності досягається за рахунок використання простих побайтових операцій замість складних обчислень. Схема є стійкою до компрометації окремих частин, оскільки для відновлення секрету необхідна наявність щонайменше порогової кількості часток.

Практична цінність розробленої схеми полягає у застосовності для розподілу великих масивів да них. Через це схема перспективна для впровадження у сфери, де критично важлива швидка обробка інформації, та є обмеження на обсяг даних, що зберігаються, зокрема, системи безпечного зберігання медіа-даних та захист критичної інфраструктури.

Ключові слова: (*k, n*)-схема, розподілення секрету, відновлення секрету, дилер, коаліція учасників, секретний ключ, перестановка байтів, зашифрування, розшифрування.

Вступ

Зростання обсягів інформації, що обробляється та зберігається у сучасних інформаційних системах, підвищує ризики її втрати або компрометації. Традиційні методи захисту даних, що базуються на шифруванні, не гарантують відновлення даних у випадку їх часткової втрати. Одним із напрямків вирішення цього завдання є використання (k, n)-схем розподілу секрету [1], що забезпечують можливість відновити дані за участі не менше ніж k учасників з n. (k, n)-схеми мають широке застосування в галузях, де критично важливе гарантування стійкості: у криптографічному збе-

ріганні ключів, у системах колективного управління доступом, у захисті медіа-даних і критичної інфраструктури.

Класичні схеми розподілу секрету базуються на різних математичних підходах до формування часток та відновлення даних. Найвідомішим прикладом є схема Шаміра [2], у якій секрет представляється як вільний член полінома степеня $k - 1$ над скінченним полем, а частки утворюються як значення цього полінома в різних точках. Перевагою методу є строгий математичний апарат і доведена інформаційна безпека, проте недоліком є значні обчислювальні витрати в роботі з великими секретами, оскільки обробка потребує арифметики у скінченних полях і розв'язанні системи рівнянь у разі відновлення даних [3].

У сучасних дослідженнях розглядаються різні напрямки вдосконалення схем розподілу секретів. Так, J. Chen та ін. [4] систематизували ґраткові підходи до побудови порогових схем і показали їх значення для криптографії та збереження чутливих даних у разі машинного навчання, але зауважили на проблему значних обчислювальних витрат. L. Harn та ін. [5], і J. Ding та ін. [6] запропонували варіанти схем зі змінним порогом, що підвищують гнучкість у керуванні доступом, проте ці рішення виявляються складними для застосування у випадках великих обсягів даних. S. Pate та ін. [7] зосередилися на підвищенні ефективності у сценаріях з великими пороговими значеннями схеми розподілу, в роботі досягнуто значного прискорення відновлення секрету, але результати подані в роботі, орієнтовані на специфічні задачі, зокрема на машинне навчання. I. Alam та ін. [8] запропонували ієрархічну схему розподілу секрету з використанням додаткових механізмів верифікації часток, що підсилює контроль і безпеку, проте ускладнює впровадження через підвищену складність конструкції. Дослідження J. Cao і X. Jinchao [9] розвинули ідею напівквантового розподілу секретів, зробивши її простішою для практичного застосування, але вона вимагає спеціалізованих технічних засобів.

У контексті застосування порогових схем до даних великого обсягу, зокрема зображень, виникають додаткові виклики, пов'язані з обсягом даних та специфічною структурою даних. У роботі [10] автори розглянули схему розподілу зображень, поєднавши операцію додавання за модулем 2 та використання шумових зображень, що значно спрощує реалізацію та знижує часові витрати. При цьому сумарний обсяг розподілених часток є значним, оскільки кожна з них містить дані, співмірні з розміром секрету.

Окремий клас становлять візуальні схеми розподілу [11], де секретне зображення поділяється на кілька прозорих шарів, і його відновлення можливе лише у разі накладання достатньої кількості таких шарів. Підхід відзначається простотою та наочністю, проте створює надлишкові дані та має обмежене практичне застосування поза сферою захисту візуальної інформації.

Попри суттєвий прогрес у вдосконаленні порогових схем, залишаються нерозв'язаними питання зменшення обсягу розподілених часток, часу обробки на розподілення та відновлення [12]. Більшість відомих методів орієнтовані на розподіл криптографічних секретних ключів, що є малими за обсягом, але непридатні для розподілу значних обсягів інформації. Тому існує потреба у нових підходах, які забезпечать ефективний розподіл та відновлення секретних даних великого обсягу без втрати основних властивостей порогової схеми. У роботі [13] пропонується метод, що дозволяє скоротити обсяг часток та знизити обчислювальні витрати, зберігаючи можливість відновлення секрету за участі визначеного порогу учасників. Саме такий метод покладено в основу досліджень у статті.

Метою роботи є зменшення обсягу розподілених даних шляхом розробки (k, n)-схеми, що передбачає використання блоків попередньо зашифрованих початкових даних.

Для досягнення мети розв'язано такі задачі:

– розробка математичної моделі (k, n)-схеми;

– дослідження обсягу розподілених даних залежно від параметрів k і n;

– експериментальне дослідження (k, n)-схеми на прикладі зображення.

Результати досліджень

(k, n)-схему часто називають пороговою схемою, оскільки параметр k визначає мінімальну кількість (поріг) учасників, які можуть відновити секрет. В моделі (k, n)-схеми ключовими поняттями є дилер та коаліція [14]. Дилер — це довірена сторона D, яка володіє секретом S і виконує процедуру генерування часток $\{P_1,...,P_n\}$. На етапі розподілу дилер відповідає за коректне формування часток відповідно до вибраної конструкції та за їхню безпечну доставку відповідним учас-

никам. В моделі з довіреним дилером припускається, що D коректний і не зловживає привілеями. Компрометація дилера змінює модель загроз і вимагає застосування додаткових механізмів. Коаліція — це будь-яка підмножина учасників $C \subseteq \{1,\ldots, n\}$. Поріг визначає критичний розмір коаліції. Якщо до складу коаліції входить k або більше учасників, то вони повинні мати достатньо інформації для відновлення S. Якщо коаліцію складають менше ніж k учасників, то в ідеальній схемі [15] сукупність розподілених часток цієї коаліції не надає жодної корисної інформації про S.

Особливість (k, n)-схеми розподілу даних, що розглядається в цій роботі, полягає в тому, що частки утворюються як сукупність блоків попередньо зашифрованого секрету S, а не як складні математичні перетворення, використовувані відомими (k, n)-схемами.

Зашифрування секрету S відбувається шляхом перестановки байтів в межах усієї множини S і заміни цих байтів. Перестановка байтів передбачає використання згенерованих псевдовипадковим чином чисел, що будуть відповідати новим номерам позицій байтів. Псевдовипадковість послідовності чисел забезпечується використанням секретного ключа. В роботі В. А. Лужецького і І. С. Горбенко [16] запропоновано узагальнений підхід до побудови таких генераторів чисел в діапазоні від 0 до $N - 1$. Основна ідея цього підходу полягає в тому, що діапазон чисел від 0 до $N - 1$ розбивається на l піддіапазонів. Якщо $b = \dfrac{N}{l}$ — ціле число, то кожний з піддіапазонів містить b чисел. Кожен піддіапазон визначається мінімальним та максимальним значенням числа

$$B_l = \left[b^l_{\min}, b^l_{\max} \right].$$

Якщо b не є цілим числом, то $(l - 1)$ піддіапазонів складаються з $\left]\dfrac{N}{l}\right[$ чисел, а l-й піддіапазон містить $N - 1(l - 1)\left]\dfrac{N}{l}\right[$ чисел.

Піддіапазон, з якого вибирається число, визначається r-розрядним двійковим кодом, що генерується регістром зсуву з лінійним зворотним зв'язком. Початковий стан регістру зсуву задається секретним ключем K_1, що забезпечує псевдовипадковість процесу генерування.

Вибір чисел з піддіапазону здійснюється детермінованим способом. При цьому формування послідовності чисел може починатися з $b^l_{\min}$ зі збільшенням числа на кожному кроці на одиницю або, починаючи з $b^l_{\max}$, зі зменшенням числа на одиницю на кожному кроці. Такі операції реалізуються на основі реверсивного лічильника СТ. Наявність двох варіантів забезпечує додаткову стійкість до зламу, оскільки для кожного з лічильників окремо визначаються початковий і кінцевий стани. Початкове значення стану лічильника визначається складовою секретного ключа $K_2 = \left\{k_{2,j}\right\}$, де $j = 0,1, \ldots, l - 1$. Наступний стан лічильника формується за таким правилом:

$$CT_j(t+1) = CT_j(t) + (-1)^{k_{2,j}},$$

де $CT_j(t)$ — стан j-го лічильника на кроці t.

Число, що вибирається з j-го піддіапазону, визначається за номером піддіапазону і станом відповідного лічильника.

$$r = j \cdot b + CT_j(t).$$

Заміна байтів (підстановка) виконується за таким правилом:

$$s_i^* = \left(s_i + z(t)\right) \bmod 256,$$

де s_i — i-й байт секрету S; $z(t) = \left(f \cdot x(t) + g \cdot x(t) + h\right) \bmod 256$.

Тут f, g, h — непарні числа, які визначаються секретним ключем K_3;

$x(t) = \left(v(t) << 8\right) \,\&\, 0xFF$, де $<<$ — циклічний зсув в ліво на 8 позицій коду стану регістру $v(t)$.

$y(t) = \left(v^*(t) << 8\right) \,\&\, 0xFF$, де $v^*(t) = \left(v(t) << 8\right)$.

Така підстановка виконує роль побайтового маскування даних. Секретний ключ K має 3 складові: K_1 — код початкового стану LFSR, K_2 — код, що визначає початковий стан лічильників і

режим їхньої роботи (додавання або віднімання 1) та K_3 — значення f, g, h. Така реалізація алгоритму шифрування забезпечує зворотне відновлення секрету шляхом використання оберненої функції підстановки, тобто віднімання за модулем 256 та такої ж послідовної перестановки.

Отже, на виході алгоритму шифрування отримуються зашифрований секрет S^*, що набуває псевдовипадкового вигляду та його відновлення без знання секретного ключа є неможливим. Подальші дії виконує дилер, який ініціює розподіл S^* серед учасників. Для цього отримані дані представляються як набір блоків, кількість яких дорівнює кількості учасників схеми розподілу

$$S^* = \left\{ s_1^*, s_2^*, ..., s_n^* \right\}.$$

Після розбиття S^* на n блоків, дилер формує частки для кожного учасника. Частка кожного учасника P_q (де $q = 1,...,n$) складається з $(n - k)$ блоків

$$P_q = \left(s_{q+j}^* \right),$$

де $j = 0,1,...,(n-k-1)$, якщо $q + j > n$, то $q = q + j - n$.

За такого складу часток, той самий блок може входити одразу до кількох часток.

Окрім формування часток, дилер обчислює власну частку

$$D = s_1^* \oplus s_2^* ... \oplus s_n^*.$$

Нехай для відновлення S^* дилеру надано k часток. Перша частка складається з $(n - k)$ блоків, а решта часток містить по одному оригінальному блоку, оскільки, інші блоки будуть повторювати блоки в інших частках. Таким чином, сумарна кількість блоків, які надаються дилеру для відновлення дорівнює $n - 1$. Блок, якого не вистачає для відновлення S^* визначається на основі власної частки дилера. Наприклад, нехай не вистачає блоку s_2^*, тоді дилер виконує такі обчислення:

$$s_2^* = D \oplus s_1^* \oplus s_3^* ... \oplus s_n^*.$$

Якщо для відновлення дилеру надано $k - 1$ часток, то сумарна кількість блоків буде дорівнювати $n - 2$. На основі власної частки дилер може визначити лише один блок, а в цьому випадку потрібно визначити 2 блоки. Тобто дилер не має можливості відновити S^* за наявності $k - 1$ часток.

Маючи всі n блоків, дилер формує S^* та розшифровує його, отримуючи початковий секрет S.

Визначимо обсяг даних, які будуть зберігати учасники та дилер для секрету обсягом C_s байт. Якщо секрет розбивається на n блоків, то обсяг блоку дорівнює $b = \frac{C_s}{n}$ байт. Враховуючи, що частка кожного учасника складається з $n - k$ блоків, то обсяг такої частки дорівнює

$$C_p = (n-k) \cdot b = (n-k) \cdot \frac{C_s}{n}.$$

Обсяг власної частки дилера дорівнює b, оскільки вона визначається як побітова сума за модулем 2 усіх блоків секрету. Таким чином обсяг даних C_a, які будуть зберігати учасники та дилер розподілу секрету, дорівнює

$$C_a = n \cdot (n-k) \cdot \frac{C_s}{n} + \frac{C_s}{n} = \frac{C_s}{n} \cdot \left(n^2 - n \cdot k + 1 \right).$$

У відомих схемах розподілу секрету, зокрема у схемі Шаміра, кожна частка за обсягом дорівнює повному секрету. Це означає, що загальний обсяг даних, який формується в результаті розподілу, дорівнює

$$C_в = C_s \cdot n.$$

Запропонована (k, n)-схема розподілу секрету, порівняно з відомими схемами, забезпечує таке зменшення обсягу даних, які потрібно передавати та зберігати:

$$\delta = \frac{C_в}{C_a} = \frac{n^2}{n^2 - n \cdot k + 1}.$$

В табл. 1 подано значення δ, для різних параметрів k та n.

Таблиця 1

Значення δ

(k,n)	(2,5)	(3,5)	(4,5)	(2,10)	(3,10)	(5,10)	(9,10)
δ	1,56	2,27	4,16	1,23	1,4	1,96	9,09

Аналіз значень δ показує, що зі зменшенням різниці $(n - k)$ запропонована схема розподілу секрету значно зменшує обсяг даних, які потрібно зберігати та передавати. Але за малих k значення δ наближається до одиниці.

Результати експериментів

На рис. 1 показано тестове зображення, а на рис. 2 — зашифроване тестове зображення та частки схеми розподілу для $k = 3$ та $n = 5$. Зашифроване зображення умовно поділене на блоки s_i^*.

Рис. 1. Тестове зображення

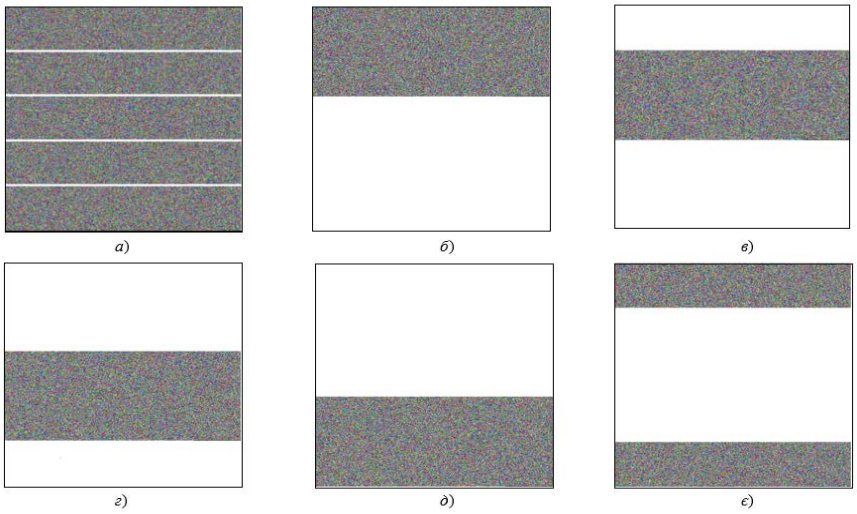

Рис. 2. Зашифроване тестове зображення:
а — схема розбиття на блоки, *б* — частка P_1, *в* — частка P_2, *г* — частка P_3, *д* — частка P_4, *є* — частка P_5

Для перевірки запропонованої (k, n)-схеми розподілу секрету проведено експерименти на прикладі кольорових зображень різних розмірів: 256×256, 512×512, 1024×1024 та 2800×1800 пікселів. Оскільки, кольорове зображення має специфічну структуру [17] через те, що кожен піксель подається сукупністю 3 байтів (R, G, B), то для зручності подальшого шифрування воно попередньо перетворюється у вектор. Далі виконується зашифрування даних та запропонована (k, n)-схема розподілу. Для тестування задано такі параметри схеми: $k = 3$, $n = 5$. Експерименти проводилися на персональному комп'ютері з процесором AMD Ryzen 5 8400F (4,2 GHz) та 32GB оперативної пам'яті. Вимірювання часу здійснювалось лише для основних обчислювальних етапів: процесу розбиття секрету на частки з урахуванням обчислення власної частки дилера, а також відновлення повного вектора секрету з наданих часток. Операції введення-виведення даних (читання і запис файлів) не включалися до вимірювань, щоб уникнути впливу зовнішніх факторів на результати.

У табл. 2 подано експериментальні дані для різних розмірів зображень. Для кожного варіанта вказано час виконання операцій та розраховану загальну пропускну здатність схеми у мегабітах за секунду (Мбіт/с).

Таблиця 2

Експериментальні дані схеми розподілу

Розмір зображення	Обсяг даних	Час зашифрування / розшифрування, с	Час розподілу / відновлення, с	Загальна пропускна здатність, Мбіт/с
256×256×3	149 KB	0,0169 / 0,0165	0,0027 / 0,0033	62,3 / 61,7
512×512×3	769 KB	0,086 / 0,085	0,0077 / 0,0083	67,2 / 67,4
1024×1024×3	3 MB	0,342 / 0,347	0,028 / 0,032	68,0 / 66,4
2800×1800×3	14,4 MB	1,64 / 1,66	0,115 / 0,159	68,7 / 66,3

Отримані результати експериментів свідчать про те, що час процесів зашифрування, розшифрування, розподілу та відновлення має лінійну залежність від розміру даних. Таким чином, запропонована (k, n)-схема демонструє передбачувану масштабованість, що дозволяє об'єктивно оцінювати її продуктивність для реальних обсягів даних. У табл. 3 подано порівняння часових витрат для виконання процесів розподілу та відновлення секретних даних обсягом 10 МВ.

Таблиця 3

Оцінка часу реалізації (3,5) схем розподілу секрету

Схема розподілу	Час розподілу, с	Пропускна здатність розподілу, Мбіт/с	Час відновлення, с	Пропускна здатність розподілу, Мбіт/с
Запропонована	1,2221	68,64	1,2619	66,48
Kamal, Fujisawa [18]	2,5762	32,56	2,3419	35,82
Ramp (RSSS) [19]	3,9281	21,36	3,6954	22,70
Shamir [20]	5,7412	14,61	5,2876	15,86

Варто зазначити, що схеми, запропоновані в роботах [18]—[20] не передбачають попереднього шифрування даних перед формуванням часток учасників коаліції. Аналіз оцінок з табл. 3 показує, що запропонована (k, n)-схема забезпечує вищу пропускну здатність порівняно з відомими схемами, як на етапі розподілу, так і у разі відновлення, демонструючи кращу масштабованість та ефективність обробки даних великого обсягу.

Висновки

Особливість запропонованої авторами (k, n)-схеми розподілу секрету полягає в тому, що попередньо реалізується зашифрування секретних даних з подальшим їх розбиттям на n блоків і формування часток для учасників коаліції. Всі ці дії виконує дилер, який також відновлює секрет з часток, що надають йому учасники коаліції. Для відновлення даних необхідна наявність щонайменше k часток, а будь-яка коаліція, менша за порогове значення, не забезпечує можливість відновити секрет дилером. Дилер має свою власну частку, яка забезпечує можливість відновлення секрету, навіть якщо коаліція надає лише $n - 1$ блоків.

У відомих схемах розподілу секрету сумарний обсяг розподілених даних в n разів більший за обсяг секрету. Проведені дослідження підтвердили, що запропонована авторами (k, n)-схема розподілу секрету забезпечує зменшення сумарного обсягу даних, які зберігають учасники коаліції. Коефіцієнт зменшення δ залежить від параметрів k і n та зростає зі збільшенням значення k.

Результати експериментальних досліджень показали, що запропонована схема демонструє передбачувану лінійну залежність складності реалізації від розміру вхідних даних, що є важливою перевагою у практичному застосуванні. Порівняльний аналіз з відомими схемами Шаміра, пороговою схемою RSSS, а також зі схемою запропонованою Kamal та Fujisawa підтверджує вищу продуктивність запропонованого авторами методу як на етапі розподілу, так і під час відновлення секрету. Зокрема, в обробці даних обсягом 10 МБ запропонована схема забезпечила найменший час виконання операцій і найвищу пропускну здатність.

Таким чином, запропонована (k, n)-схема розподілу секрету поєднує властивості відомих порогових схем з можливістю масштабованого застосування у сценаріях обробки великих обсягів даних зі зменшенням обсягу розподілених часток та швидкої обробки даних, що вказує на перспективу її подальшого дослідження та реалізації.

Подальші дослідження можуть бути спрямовані на розширення застосовування схеми у сценаріях з динамічними параметрами (k, n), розробку механізму перевірки автентичності часток, а також інтеграцію у сучасні криптографічні протоколи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] B. Amos, *Secret-Sharing Schemes for General Access Structures: An Introduction*, University of the Negev Beer-Sheva, Israel, pp. 10-15, Mar. 2025.[Electronic resource]. Available: https://eprint.iacr.org/2025/ 518.pdf .

[2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979. https://doi.org/10.1145/359168.359176 .

[3] M. Naor, and A. Shamir, "Visual cryptography," in *Advances in Cryptology - EUROCRYPT 94, Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1994. https://doi.org /10.1007/BFb0053419 .

[4] J. Chen, et al., "Lattice-Based Threshold Secret Sharing Scheme and Its Applications: A Survey," *Electronics*, vol. 13,

no. 2, p. 287, Jan. 2024. https://doi.org /10.3390 /electronics13020287 .

[5] L. Harn, et al., "A Novel Threshold Changeable Secret Sharing Scheme," *Frontiers of Computer Science*, vol. 16, no. 1, p. 161807, Feb. 2022. https://doi.org/10.1007/s11704-020-0300-x .

[6] D. Jian, et al., "Full Threshold Change Range of Threshold Changeable Secret Sharing," *Designs, Codes and Cryptography*, vol. 91, no. 7, pp. 2421-47, Jul. 2023. https://doi.org /10.1007/s10623-023-01205-9 .

[7] S. Patel, et al., "Efficient Secret Sharing for Large-Scale Applications," *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* [Salt Lake City UT USA], pp. 3065-79, 2024. https://doi.org/10.1145/3658644.3670379 .

[8] A. Irfan, et al., "A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structure," *Axioms*, vol. 13, no. 8, p. 515, Jul. 2024. https://doi.org /10.3390/axioms13080515 .

[9] C. Jie, and J. Xu, "Efficient (k, n) Threshold Semi-Quantum Secret Sharing Protocol," *Frontiers in Physics*, vol. 13, Feb. 2025. https://doi.org/10.3389/fphy.2025.1542675 .

[10] L. Cheng-Shian, et al., "XOR-Based Progressively Secret Image Sharing," *Mathematics*, vol. 9, no. 6, p. 612, Mar. 2021. https://doi.org/10.3390 /math9060612 .

[11] R. I. Dyala, J. S. Teh, and R. Abdullah, "An overview of visual cryptography techniques," *Multimed Tools Appl*., vol. 80, pp. 31927-31952, 2021. https://doi.org /10.1007/s11042-021-11229-9 .

[12] K. Arup, et al., "Secret Sharing: A Comprehensive Survey, Taxonomy and Applications," *Computer Science Review*, vol. 51 p. 100608, Feb. 2024, https: //doi.org/10.1016 /j.cosrev.2023.100608 .

[13] В. А. Лужецький, і М. С. Ціхоцький, «Схема порогового розподілення секрету (k, n),» *ІТКМ IEEE*, Івано-Франківськ, сек. 5(24), с. 147-148, Травня. 2024. ISBN 978-966-640-560-2.

[14] P. D'arco, R. Prisco, and A. Santis, "Secret Sharing Schemes for Infinite Sets of Participants: A New Design Technique," *Theoretical Computer Science*, vol. 859, pp. 149-61, Mar. 2021. https://doi.org /10.1016/j.tcs.2021.01.019 .

[15] Beimel, A., and B. Chor. "Universally Ideal Secret-Sharing Schemes," *IEEE Transactions on Information Theory*, vol. 40, no. 3, pp. 786-94, May 1994. https://doi.org/10.1109/18.335890 .

[16] В. А. Лужецький і І. С. Горбенко, «Метод формування перестановок довільної кількості елементів,» *Інформаційна безпека*, № 15, № 3, с. 262-67, 2013.

[17] L. Wendan, et al., "A Reversible and Lossless Secret Image Sharing Scheme with Authentication for Color Images," *Journal of King Saud University — Computer and Information Sciences*, vol. 35, no. 10, p. 101854, Dec. 2023. https://doi.org/10.1016/j.jksuci.2023.101854 .

[18] A. Kamal, and M. Fujisawa, "Efficient and Secure Secret Sharing-Based Data Outsourcing Suitable for Internet of Things Environments," *Internet of Things*, vol. 32, p. 101645, Jul. 2025. https://doi.org/10.1016/j.iot.2025.101645 .

[19] D. Bogdanov, "Foundations and properties of Shamir's secret sharing scheme Research Seminar in Cryptography," *University of Tartu, Institute of Computer Science*, pp. 10, May. 2007. https://researchgate.net/publication/254446884 .

[20] G. Olav, "Considerate Ramp Secret Sharing," *Arxiv*, Department of Mathematical Sciences Aalborg University, p. 12, Aug. 2025. https://arxiv.org/html/2412.17987v3 .

Рекомендована кафедрою захисту інформації ВНТУ

Стаття надійшла до редакції 22.09.2025

Лужецький Володимир Андрійович — д-р техн. наук, професор, завідувач кафедри захисту інформації, e-mail: lva.kzi2002@gmail.com ;

Ціхоцький Микита Сергійович — аспірант кафедри захисту інформації, e-mail: nik.tsikhotskiy15@gmail.com .

Вінницький національний технічний університет, Вінниця

V. A. Luzhetskyi[1]
M. S. Tsikhotskyi[1]

Secret Sharing of Encrypted Data Using a (k, n)-Scheme Based on Encrypted Blocks

[1]Vinnytsia National Technical University

In this paper, we present a threshold secret sharing scheme designed for the large-scale data, which are pre-encrypted prior to distribution. The relevance of this research stems from the continuous growth of data volumes processed in modern information systems, which imposes additional requirements on existing secret sharing schemes. Traditional secret sharing approaches, despite their solid theoretical foundation and proven information-theoretic security, demand significant computational resources due to the use of complex mathematical operations and are primarily tailored for small-sized secrets (e.g.,

cryptographic keys). Consequently, they are poorly suited for protecting large datasets. Furthermore, in such schemes the volume of distributed shares may substantially exceed the size of the original data.

The objective of this work is to reduce the overall volume of distributed data by designing a (k, n) secret sharing scheme that operates on pre-encrypted blocks of the original dataset.

The distinguishing feature of the proposed (k, n)-scheme lies in the integration of a preliminary encryption stage, followed by splitting the encrypted data into n blocks and generating shares for coalition participants. All these operations are performed by the dealer, who is also responsible for reconstructing the secret from the shares provided by coalition members. At least k shares are required for secret reconstruction, while any coalition smaller than the threshold is unable to recover the secret. The dealer additionally retains a dedicated share, which ensures the possibility of secret recovery even if the coalition provides only n − 1 blocks.

In conventional secret sharing schemes, the cumulative size of the distributed data is typically n times greater than the size of the secret. Experimental results confirm that the proposed (k, n)-scheme reduces the cumulative storage requirements for coalition participants. The reduction factor δ depends on the values of k and n, and increases as k grows.

The proposed scheme exhibits linear time complexity with respect to the input data size, which represents a significant advantage for practical deployment. Compared to well-known threshold secret sharing methods, the scheme achieves higher performance. The performance gain is attained by employing simple byte-wise operations instead of computationally intensive procedures. Moreover, the scheme is resilient to partial compromise, since secret recovery requires the presence of at least the threshold number of shares.

The practical value of the developed scheme lies in its applicability to large-scale data distribution. This makes it a promising solution for domains where rapid data processing and storage efficiency are critical, including secure media storage systems and the protection of critical infrastructure.

Keywords: (*k*, *n*)-scheme, secret sharing, secret reconstruction, dealer, participant coalition, secret key, byte permutation, encryption, decryption.

Luzhetskyi Volodymyr A. — Dr. Sc. (Eng.), Professor, Head of the Chair of Information Security, e-mail: lva.kzi2002@gmail.com ;

Tsikhotskyi Mykyta S. — Post-Graduate Student of the Chair of Information Security, e-mail: nik.tsikhotskiy15@gmail.com