ISSN 0485-8972

УДК 004.056:519.2 **DOI:10.30837/rt.2026.1.224.03**

А.М. ОЛЕКСІЙЧУК, д-р техн. наук, М.І. ПОКИДКО

РІВНОМІРНО РОБАСТНА ПОРОГОВА СХЕМА РОЗДІЛЕННЯ СЕКРЕТУ ДЛЯ МАКСИМАЛЬНОГО ЗНАЧЕННЯ ПОРОГУ З МЕНШИМИ СКЛАДНОСТЯМИ ОБЧИСЛЕННЯ ПРОЄКЦІЙ ТА ВІДНОВЛЕННЯ СЕКРЕТУ

Вступ

Схема розділення секрету (СРС) являє собою криптографічний протокол, який надає змогу "розподіляти" секрет серед учасників $1, 2, ..., n$ таким чином, щоб тільки певні (*дозволені*) коаліції учасників мали можливість відновлювати значення секрету при об'єднанні своїх компонент (*проєкцій секрету*). Сукупність усіх дозволених коаліцій учасників називається *структурою доступу* зазначеної СРС.

СРС поділяють на безумовно стійкі та обчислювально стійкі. Перші виключають можливість отримання повної інформації про секрет учасниками будь-якої *забороненої* коаліції (тобто такої, що не входить до структури доступу). Стійкість зазначених СРС не залежить від припущень про обчислювальні можливості учасників. Обчислювально стійкі СРС забезпечують неможливість практичного відновлення секрету учасниками заборонених коаліцій за умови, що останні мають обмежені обчислювальні ресурси. СРС називається *досконалою*, якщо будь-яка заборонена коаліція учасників не може отримати жодної апостеріорної інформації про значення секрету, та *недосконалою* – у протилежному випадку. На сьогодні література, присвячена СРС та їх застосуванням, налічує тисячі найменувань. Відзначимо оглядову роботу [1], де можна знайти подальші посилання.

Найвідомішим прикладом досконалої СРС є (k, n)-порогова схема Шаміра [2], структура доступу якої складається з усіх коаліцій, які містять не менше ніж k з n учасників. Секрети у схемі Шаміра є елементами скінченного поля F порядку $q > n$. При цьому i-й учасник отримує несекретний ідентифікатор $x_i \in F \setminus \{0\}$, де $x_i \neq x_j$ при $i \neq j$, $i, j \in \overline{1,n}$. Для розділення секрету $s_0 \in F$ адміністратор СРС (або *дилер*) вибирає випадковий рівноймовірний поліном $f(x)$ степеня $\deg f(x) \leq k-1$ над полем F такий, що $f(0) = s_0$. Далі він передає захищеним каналом зв'язку i-му учаснику СРС проєкцію $s_i = f(x_i)$, $i \in \overline{1,n}$. Будь-яка коаліція з k або більше учасників може відновити поліном $f(x)$, а отже і секрет s_0, за відповідним набором проєкцій, використовуючи інтерполяційну формулу Лагранжа, в той час як будь-яка заборонена коаліція (з менше ніж k учасників) не має про секрет жодної апостеріорної інформації [2, 3].

В [4] показано, що схема Шаміра є нестійкою до атаки з боку "нечесних" учасників (cheaters), які можуть підміняти власні проєкції для того, щоби спотворити значення секрету при відновленні. Більш точно: нехай "нечесні" учасники $i_1,...,i_{k-1}$ подають на вхід алгоритму відновлення секрету елементи $s'_{i_1},...,s'_{i_{k-1}}$ поля F замість $s_{i_1},...,s_{i_{k-1}}$ відповідно. Мета атаки полягає в тому, щоб при отриманні проєкції s_{i_k} від будь-якого "чесного" учасника i_k алгоритм відновлення секрету видав би деяке значення $s' \neq s_0$ за вхідними даними $s'_{i_1},...,s'_{i_{k-1}}, s_{i_k}$. Для протидії цій атаці в [4] запропоновано дві модифікації у схемі Шаміра, перша з яких полягає в зменшенні сукупності секретних ключів до власної підмножини S поля F, а друга – у засекречуванні ідентифікаторів учасників. Згідно з [4] секрет s_0 вибирається навмання з множини S потужності $l < q$, а i-й учасник отримує від дилера пару (x_i, s_i) захищеним каналом зв'язку, $i \in \overline{1,n}$. В [4] показано, що (навіть за умови знання секрету) ймовірність

успішного проведення атаки, тобто отримання на виході алгоритму відновлення секрету деякого елемента $s' \in S \setminus \{s_0\}$, не перевищує $(l-1)(k-1)(q-k)^{-1}$ і може бути зроблена як завгодно малою при фіксованих k та l за рахунок вибору достатньо великого значення q.

Робота [4] викликала помітний інтерес до побудови різноманітних конструкцій СРС, що є стійкими до атаки підміни проєкцій (згодом такі СРС отримали назву *робастних*). Певним підсумком досліджень в цьому напрямі можна вважати статті [5–7]. Зокрема, в [6] отримано нижню оцінку обсягу секретних даних, що мають зберігати учасники СРС, для якого ймовірність успішної підміни проєкцій довільною забороненою коаліцією "нечесних" учасників не перевищує заданого числа $\delta < 1$. Описано також конструкцію, яка за певної умови дозволяє будувати порогові СРС, для яких досягається зазначена оцінка. Ця умова полягає в існуванні простого числа q та планарної різницевої множини потужності l, тобто такої множини $S \subset \overline{0, q-1}$, де $|S| = l$, що для кожного $a \in \overline{1, q-1}$ є точно одна пара $(s, s') \in S \times S$ з властивістю $a = (s - s') \bmod q$. Згідно з [6] для побудови робастної СРС достатньо скористатися схемою Шаміра для множини секретів, що дорівнює S. В [7] запропоновано використовувати для побудови робастних (не обов'язково порогових) СРС так звані AMD-коди, зводячи задачу до побудови спеціальних випадкових відображень множини секретів у більш потужну множину (скінченне поле або скінченну абелеву групу). Відомості про подальший прогрес в цьому напрямі можна знайти в [8].

Зауважимо, що наведені у [5–8] та деяких інших публікаціях конструкції робастних СРС базуються виключно на відображеннях зазначеного типу. А саме, з метою побудови робастної СРС для множини секретів S певним чином вибирають її ін'єктивне відображення в більш потужну множину секретів для заздалегідь вибраної досконалої (не обов'язково робастної) СРС. Саме властивості цього відображення, яке задається за допомогою AMD-коду [7] або шляхом ототожнення S з планарною різницевою множиною [6] (або якось інакше [5]), гарантують робастність схеми, що будується, в той час як на допоміжну СРС не накладається жодних обмежень.

Незважаючи на привабливість та простоту відзначеного підходу, слід зауважити, що створені подібним чином СРС (на відміну від першої робастної СРС [4]) не є *рівномірно робастними*, тобто стійкими до підміни проєкцій з боку "нечесних" учасників незалежно від вибору підмножини S в більш потужній сукупності секретів. Можливі застосування рівномірно робастних СРС заслуговують окремого дослідження. Зазначимо лише, що їх можна використовувати для автентифікації джерела секретних ключів (тобто дилера) шляхом передачі поряд із секретом певної перевірочної інформації без додаткового збільшення довжини повідомлень, які подаються на вхід допоміжної СРС.

Мета статті – побудова рівномірно робастної досконалої порогової СРС з максимальною величиною порогу $k = n$, яка характеризується меншими часовими складностями обчислення проєкцій та відновлення секрету в порівнянні з відомою рівномірно робастною СРС [4]. Інтерес до таких схем обумовлений, головним чином, можливістю будувати на їх основі досконалі СРС для довільних структур доступу, що виявляється прийнятним для практичних застосувань за умови, що кожен учасник входить до не надто великої кількості мінімальних дозволених коаліцій (див., наприклад, [3]). Показано, що обсяг даних, які зберігають учасники запропонованої СРС, збігається з тим, що мають учасники схеми з [4]. При цьому виграш у складності обчислень становить приблизно k разів.

Постановка задачі та отримані результати

Побудуємо рівномірно робастну досконалу (k, k)-порогову СРС, яка характеризується меншими складностями обчислення проєкцій та відновлення секрету в порівнянні з СРС, описаною в [4].

Нехай секрет вибирається навмання з деякої (довільної) множини S потужності l, яка міститься у скінченному полі F порядку q.

Для розподілу секрету $s_0 \in S$ *дилер виконує такі дії*:

1) генерує незалежні випадкові рівноймовірні елементи $a_1,...,a_{k-1} \in F$, $b \in F \setminus \{0\}$;

2) генерує незалежні випадкові рівноймовірні елементи $r_1,...,r_{k-1} \in F$ та обчислює вектор

$$(s_0, s_1,..., s_k) = (s_0, r_1,..., r_{k-1})G, \tag{1}$$

де

$$G = \begin{pmatrix} 1 & a_1 & \dots & a_{k-1} & b + (a_1 + \dots + a_{k-1}) \\ 0 & 1 & \dots & 0 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 1 \end{pmatrix}; \tag{2}$$

3) передає i-му учаснику захищеним каналом зв'язку елемент a_i та проєкцію s_i, $i \in \overline{1, k-1}$;

4) передає k-му учаснику захищеним каналом зв'язку елемент $a_k = b + (a_1 + ... + a_{k-1})$ та проєкцію s_k.

З вигляду матриці (2) випливає, що її рядки породжують максимально дистанційно роздільний код довжини $k+1$ та вимірності k над полем F; отже, усі k учасників можуть однозначно відновити секрет, а будь-яка коаліція з $k-1$ учасників не має про нього жодної апостеріорної інформації (див. теорему 3.1 в [8]).

Алгоритм відновлення секрету отримує на вхід елементи a_i, s_i ($i \in \overline{1, k}$), після чого обчислює значення $b = a_k - (a_1 + ... + a_{k-1})$ та перевіряє умову $b \neq 0$. Якщо вона не виконується, то алгоритм сигналізує про некоректність вхідних даних і завершує роботу. У протилежному випадку він обчислює секрет за формулою

$$s_0 = b^{-1}(s_k - (s_1 + \dots + s_{k-1})), \tag{3}$$

та перевіряє умову $s_0 \in S$. Алгоритм завершується успішно тільки за цієї умови. Зауважимо, що його коректність випливає безпосередньо з рівностей

$$s_i = s_0 a_i + r_i,\ i \in \overline{1, k-1},\ s_k = s_0 a_k + (r_1 + ... + r_{k-1}), \tag{4}$$

які є наслідками формул (1) і (2).

Припустимо, що учасники $1, 2, ..., k-1$ є "нечесними" та намагаються підмінити дані, отримані від дилера, з метою спотворення секрету s_0 при його відновленні. Для цього вони вибирають елементи $a'_1,...,a'_{k-1} \in F$, $s'_1,...,s'_{k-1} \in F$ так, щоб алгоритм відновлення секрету видав би деяке значення $s' \in S$, відмінне від s_0, за вхідними даними $a'_1,...,a'_{k-1}, a_k$, $s'_1,...,s'_{k-1}, s_k$, де елементи a_k та s_k подає "чесний" k-й учасник.

Розглянемо ймовірнісний простір, який складається з усіх можливих наборів значень незалежних випадкових елементів $a_1,...,a_{k-1} \in F$, $b \in F \setminus \{0\}$, $r_1,...,r_{k-1} \in F$, $s_0 \in S$, розподілених рівномірно на зазначених множинах. Позначимо символом R алгоритм відновлення секрету, символом α – набір даних, які отримують від дилера учасники $1, 2, ..., k-1$, а символом β – набір даних, які подають учасники $1, 2, ..., k$ на вхід алгоритму R: $\alpha = (\hat{a}_i, \hat{s}_i : i \in \overline{1, k-1})$, $\beta = (a'_i, a_k, s'_i, s_k : i \in \overline{1, k-1})$.

Стійкість описаної СРС до підміни даних з боку учасників $1, 2, ..., k-1$ характеризується набором умовних ймовірностей

$$p_{\alpha,\beta} = \Pr\left(R(\beta) \in S \setminus \{s_0\} \mid (a_i, s_i : i \in \overline{1,k-1}) = \alpha\right), \quad (5)$$

які визначаються (відносно зазначеного ймовірнісного простору) для наведених вище значень α, β.

Як показує наступне твердження, усі ймовірності (5) можна зробити як завгодно малими, вибираючи належним чином значення q для заданого числа $l = |S|$.

Т в е р д ж е н н я 1. Для будь-яких можливих значень α, β виконується нерівність

$$p_{\alpha,\beta} \le l(q-1)^{-1}.$$

Д о в е д е н н я. Зафіксуємо елементи $\hat{a}_i, \hat{s}_i \in F$ $(i \in \overline{1,k-1})$ та розглянемо подію $W = \bigcap_{i=1}^{k-1} \{a_i = \hat{a}_i, s_i = \hat{s}_i\}$. Використовуючи формулу (4) та незалежність і рівноймовірність випадкових елементів a_i, r_i, s_0, $i \in \overline{1,k-1}$, отримаємо, що $\Pr(W) = q^{-2(k-1)}$. Окрім того, згідно з формулою (5) виконуються такі рівності:

$$p_{\alpha,\beta} = \Pr(\{R(\beta) \in S \setminus \{s_0\}\} \cap W)(\Pr(W))^{-1} = (\Pr(W))^{-1} \sum_{s' \in S} \Pr(\{R(\beta) = s', s_0 \ne s'\} \cap W). \quad (6)$$

Для кожного $s' \in S$ отримаємо вираз випадкової величини $R(\beta)$ за умови реалізації події W. На підставі означення алгоритму R справедлива рівність

$$R(\beta) = \tilde{b}^{-1}(s_k - (s'_1 + \cdots + s'_{k-1})),$$

де

$$\tilde{b} = a_k - (a'_1 + ... + a'_{k-1}) = b + (\hat{a}_1 + ... + \hat{a}_{k-1}) - (a'_1 + ... + a'_{k-1}), \quad (7)$$

$$s_k = s_0 a_k + (r_1 + ... + r_{k-1}) = s_0 \tilde{b} + s_0(a'_1 + ... + a'_{k-1}) + (r_1 + ... + r_{k-1}).$$

Звідси випливає, що

$$R(\beta) = s_0 + \tilde{b}^{-1}(s_0(a'_1 + ... + a'_{k-1}) + (r_1 + ... + r_{k-1}) - (s'_1 + \cdots + s'_{k-1})).$$

Нарешті, враховуючи рівності $\hat{s}_i = s_0 \hat{a}_i + r_i$, $i \in \overline{1,k-1}$, отримаємо, що

$$\{R(\beta) = s'\} \cap W = \left(\bigcap_{i=1}^{k-1} \{a_i = \hat{a}_i, r_i = \hat{s}_i - s_0 \hat{a}_i\}\right) \cap$$

$$\cap \{s_0 + \tilde{b}^{-1}(s_0(a'_1 + ... + a'_{k-1}) + (r_1 + ... + r_{k-1}) - (s'_1 + \cdots + s'_{k-1})) = s'\}.$$

На підставі незалежності та рівноймовірності випадкових елементів a_i, r_i, s_0, $i \in \overline{1,k-1}$, з останньої рівності випливає, що

$$\Pr(\{R(\beta) = s', s_0 \ne s'\} \cap W) = \Pr(W) \mid S \mid^{-1} \sum_{\hat{s}_0 \in S \setminus \{s'\}} \Pr(\tilde{b}^{-1}(c_1 \hat{s}_0 + c_2) = s' - \hat{s}_0),$$

де

$$c_1 = (a'_1 + ... + a'_{k-1}) - (\hat{a}_1 + ... + \hat{a}_{k-1}),\ c_2 = (\hat{s}_1 - s'_1) + \cdots + (\hat{s}_{k-1} - s'_{k-1}).$$

При цьому на підставі формули (7) та рівномірності розподілу випадкової величини b на множині $F \setminus \{0\}$ ймовірність події $\tilde{b}^{-1}(c_1 \hat{s}_0 + c_2) = s' - \hat{s}_0$ дорівнює нулю або $(q-1)^{-1}$ для будь-яких $c_1, c_2 \in F$ та $\hat{s} \ne s'$. Отже,

$$\Pr(\{R(\beta) = s', s_0 \ne s'\} \cap W) \le \Pr(W)(q-1)^{-1}.$$

Підставляючи наведену оцінку в формулу (6), отримаємо нерівність $p_{\alpha,\beta} \le l(q-1)^{-1}$.

Твердження доведено.

Розглянемо випадок, в якому "нечесними" є всі учасники за винятком i-го, де $i \in \overline{1,k-1}$, та доведемо, що в цьому випадку виконується твердження, аналогічне доведеному.

Не обмежуючи загальності міркувань, вважатимемо далі, що $i=1$. Розглянемо набори даних $\alpha = (\hat{a}_i, \hat{s}_i : i \in \overline{2,k})$ та $\beta = (a_1, s_1, a_i', s_i' : i \in \overline{2,k})$, які отримають учасники $2, ..., k$ від дилера та подадуть усі учасники СРС на вхід алгоритму R відповідно, та визначимо умовні ймовірності:

$$\tilde{p}_{\alpha,\beta} = \Pr\left(R(\beta) \in S \setminus \{s_0\} \mid (a_i, s_i : i \in \overline{2,k}) = \alpha\right). \tag{8}$$

Т в е р д ж е н н я 2. Для будь-яких можливих значень α, β виконується нерівність

$$\tilde{p}_{\alpha,\beta} \le l(q-1)^{-1}.$$

Д о в е д е н н я. Позначимо $\tilde{W}$ подію $(a_i, s_i : i \in \overline{2,k}) = \alpha$. Використовуючи рівності $\hat{s}_i = s_0 \hat{a}_i + r_i$, $i \in \overline{2,k-1}$, $\hat{s}_k = s_0 \hat{a}_k + (r_2 + ... + r_{k-1}) + r_1$, $\hat{a}_k = b + (\hat{a}_2 + ... + \hat{a}_{k-1}) + a_1$, на підставі незалежності та рівноймовірності випадкових елементів a_i, r_i, s_0, $i \in \overline{1,k-1}$ отримаємо, що $\Pr(\tilde{W}) = q^{-2(k-1)}$. Окрім того, згідно з формулою (8)

$$\tilde{p}_{\alpha,\beta} = (\Pr(\tilde{W}))^{-1} \sum_{s' \in S} \Pr(\{R(\beta) = s', s_0 \ne s'\} \cap \tilde{W}). \tag{9}$$

Для кожного $s' \in S$ отримаємо вираз випадкової величини $R(\beta)$ за умови реалізації події $\tilde{W}$. На підставі означення алгоритму R справедлива рівність

$$R(\beta) = \tilde{b}^{-1}(s_k' - (s_2' + \cdots + s_{k-1}') - s_1),$$

де

$$\tilde{b} = a_k' - (a_2' + ... + a_{k-1}') - a_1,\ s_1 = s_0 a_1 + r_1 = -s_0(\tilde{b} - a_k' + (a_2' + ... + a_{k-1}')) + r_1.$$

Отже,

$$R(\beta) = s_0 + \tilde{b}^{-1}(s_0 c_1 + r_1 + c_2),$$

де $c_1 = -a_k' + (a_2' + ... + a_{k-1}')$, $c_2 = s_k' - (s_2' + \cdots + s_{k-1}')$.

Використовуючи останню рівність, отримаємо, що

$$\{R(\beta) = s'\} \cap \tilde{W} = \left(\bigcap_{i=2}^{k-1} \{a_i = \hat{a}_i, r_i = \hat{s}_i - s_0 \hat{a}_i\} \right) \cap$$

$$\cap \{\hat{s}_k = s_0 \hat{a}_k + (r_2 + ... + r_{k-1}) + r_1,\ \hat{a}_k = b + (\hat{a}_2 + ... + \hat{a}_{k-1}) + a_1,\ \tilde{b}^{-1}(s_0 c_1 + r_1 + c_2) = s' - s_0\}.$$

Позначаючи $\hat{r}_1(s_0)$ значення випадкової величини r_1, яке вона приймає за умови

$$\hat{s}_k = s_0 \hat{a}_k + (r_2 + ... + r_{k-1}) + r_1,\ r_i = \hat{s}_i - s_0 \hat{a}_i,\ i \in \overline{2,k-1},$$

отримаємо звідси, що

$$\Pr(\{R(\beta) = s', s_0 \ne s'\} \cap \tilde{W}) =$$

$$= q^{-2(k-2)} \mid S \mid^{-1} \sum_{\hat{s}_0 \in S \setminus \{s'\}} \Pr(r_1 = \hat{r}_1(\hat{s}_0), \hat{a}_k = b + (\hat{a}_2 + ... + \hat{a}_{k-1}) + a_1, \tilde{b}^{-1}(\hat{s}_0 c_1 + \hat{r}_1(\hat{s}_0) + c_2) = s' - \hat{s}_0) =$$

$$= q^{-2(k-2)} q^{-1} \mid S \mid^{-1} \sum_{\hat{s}_0 \in S \setminus \{s'\}} \Pr(\hat{a}_k = b + (\hat{a}_2 + ... + \hat{a}_{k-1}) + a_1, \tilde{b}^{-1}(\hat{s}_0 c_1 + \hat{r}_1(\hat{s}_0) + c_2) = s' - \hat{s}_0).$$

Оскільки $\tilde{b} = a_k' - (a_2' + ... + a_{k-1}') - a_1$, де випадкова величина a_1 має рівномірний розподіл на полі F, і при цьому випадкова величина b не залежить від a_1 та рівномірно розподілена на множині $F \setminus \{0\}$, то

$$\Pr(\hat{a}_k = b + (\hat{a}_2 + ... + \hat{a}_{k-1}) + a_1, \tilde{b}^{-1}(\hat{s}_0 c_1 + \hat{r}_1(\hat{s}_0) + c_2) = s' - \hat{s}_0) = q^{-1}(q-1)^{-1}N,$$

де N дорівнює числу розв'язків $(x, y) \in F \times F \setminus \{0\}$ системи рівнянь

$$\hat{a}_k = y + (\hat{a}_2 + ... + \hat{a}_{k-1}) + x, (a'_k - (a'_2 + ... + a'_{k-1}) - x)^{-1}(\hat{s}_0 c_1 + \hat{r}_1(\hat{s}_0) + c_2) = s' - \hat{s}_0,$$

де $s' - \hat{s}_0 \neq 0$. Але така система рівнянь має не більше одного розв'язку.

Отже, $\Pr(\{R(\beta) = s', s_0 \neq s'\} \cap \tilde{W}) \leq \Pr(W)(q-1)^{-1}$, звідки на підставі формули (9) випливає $\tilde{p}_{\alpha,\beta} \leq l(q-1)^{-1}$.

Твердження доведено.

У табл. 1 наведено результати порівняння запропонованої СРС з раніше відомою рівномірно робастною СРС (для випадку, коли остання має максимальну величину порогу $k = n$) [4].

Як видно з табл. 1, обидві схеми характеризуються порівнянними значеннями ймовірності успішного спотворення проєкцій "нечесними" учасниками та однаковим обсягом даних, які отримує кожен учасник від дилера. При цьому для розділення секрету в запропонованій схемі треба виконати k множень та $2k-2$ додавань в полі з q елементів, в той час як для схеми з [4] кількість як множень, так і додавань становить $k^2 - k$. Аналогічні результати мають місце і для складності відновлення секрету в обох схемах.

Таблиця 1

Порівняння рівномірно робастних СРС за ефективністю

Показник ефективності СРС	СРС з [4]	Запропонована СРС
Верхня оцінка ймовірності спотворення секрету коаліцією "нечесних" учасників	$(l-1)(k-1)(q-k)^{-1}$	$l(q-1)^{-1}$
Максимальний розмір даних (у бітах), які зберігає окремий учасник	$2\lceil \log q \rceil$	$2\lceil \log q \rceil$
Кількість операцій (множень, додавань), які виконуються при розділенні секрету	$(k^2 - k, k^2 - k)$	$(k, 2k-2)$
Кількість операцій (множень, обернень. додавань), які виконуються при відновленні секрету	$(k(2k-3), k(k-1), k^2 - 1)$	$(1, 1, k-1)$

На завершення розглянемо приклад, який ілюструє спосіб практичного застосування запропонованої СРС.

Нехай треба побудувати робастну досконалу СРС на множині учасників $M = \{1, 2, ..., 28\}$ для структури доступу, яка визначається трьома мінімальними дозволеними коаліціями: $M_1 = \{1, 2, ..., 10\}$, $M_2 = \{10, 11, ..., 19\}$, $M_2 = \{19, 20, ..., 28\}$. Іншими словами, будь-яка коаліція $A \subseteq M$ має право на відновлення секрету тоді й тільки тоді, коли вона містить хоча б одну з множин M_1, M_2, M_3. Припустимо, що секрети є двійковими векторами довжини 256, а допустима верхня межа ймовірності спотворення проєкцій "нечесними" учасниками становить 2^{-127}.

Покладемо $q = 2^{256+128} = 2^{384}$ та задамо звичайним чином поле F порядку q за допомогою незвідного полінома ступеня 384 над полем з двох елементів. Тоді елементи поля F ототожнюються з двійковими векторами довжини 384. Нарешті, задамо множину $S = \{(x_1, ..., x_{384}) \in F : x_{257} = \cdots = x_{384} = 0\}$ та скористаємося для розділення довільного секрету $s_0 \in S$ запропонованою схемою, використовуючи її окремо для кожної з трьох коаліцій M_1, M_2, M_3.

В результаті учасники коаліції M_1 отримають від дилера пари елементів $(a_i^{(1)}, s_i^{(1)})$, $i \in M_1$, учасники коаліції M_2 – пари $(a_i^{(2)}, s_i^{(2)})$, $i \in M_2$, а учасники коаліції M_3 – пари $(a_i^{(3)}, s_i^{(3)})$, $i \in M_3$, сформовані згідно з алгоритмом розділення секрету для запропонованої

(k,k)-порогової СРС при $k=10$. Кожен учасник зберігатиме одну таку пару, за виключенням учасників 10 та 19, кожен з яких зберігатиме дві такі пари.

Для відновлення секрету учасникам будь-якої дозволеної коаліції A треба знайти найменший номер $j \in \overline{1,3}$ такий, що $A \supseteq M_j$ та скористатися алгоритмом відновлення секрету в запропонованій СРС на множині M_j. Якщо кожна з множин M_1, M_2, M_3 містить хоча б одного "чесного" учасника, то на підставі тверджень 1, 2 ймовірність успішного спотворення проєкцій "нечесними" учасниками є менше за 2^{-127}.

В цілому, для розділення секрету дилеру потрібно виконати $3k=30$ множень та $6(k-2)=48$ додавань в полі порядку 2^{384}, в той час як застосування для цього СРС з роботи [4] потребуватиме $3(k^2-k)=270$ множень та стільки ж додавань.

Висновки

Запропонована СРС не поступається раніше відомій рівномірно робастній СРС [4] за жодним показником ефективності, помітно перевершуючи останню за складністю процедур розділення та відновлення секрету (див. табл. 1). Запропонована СРС будується на основі (випадкового) максимально роздільно дистанційного коду довжини $k+1$ та вимірності k над полем з q елементів, якій відрізняється від коду Ріда–Соломона, що лежить в основі конструкції з [4]. Саме це надає змогу зменшити часову складність, не збільшуючи розмір даних, які зберігають учасники, або ймовірність успішної підміни проєкцій з боку "нечесних" учасників СРС.

Запропоновану схему можна використовувати для побудови рівномірно робастних досконалих СРС, які реалізують довільні структури доступу, за умови, що кожен учасник входить до не надто великої кількості мінімальних дозволених коаліцій.

Список літератури

1. Chattopadhyay A. K. et al. Secret sharing: A comprehensive survey, taxonomy and applications // Computer Science Review. 2024. Vol. 51. Art. 100608.
2. Shamir A. How to share a secret // Communications of the ACM. 1979. Vol. 22, № 11. P. 612–613.
3. Beimel A. Secret-sharing schemes: A survey // Proceedings of the International Conference on Coding and Cryptology. Berlin ; Heidelberg : Springer, 2011. P. 11–46.
4. Tompa M., Woll H. How to share a secret with cheaters // Journal of Cryptology. 1989. Vol. 1, № 3. P. 133–138.
5. Cabello S., Padró C., Sáez G. Secret sharing schemes with detection of cheaters for a general access structure // *Designs, Codes and Cryptography*. 2002. Vol. 25, № 2. P. 175–188.
6. Ogata W., Kurosawa K., Stinson D. R. Optimum secret sharing scheme secure against cheating // SIAM Journal on Discrete Mathematics. 2006. Vol. 20, № 1. P. 79–95.
7. Cramer R., Dodis Y., Fehr S., Padró C., Wichs D. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors // Advances in Cryptology – EUROCRYPT 2008 : Lecture Notes in Computer Science. 2008. Vol. 4965. P. 471–488.
8. Stinson D. R. Combinatorial designs and cryptography, revisited // 50 Years of Combinatorics, Graph Theory, and Computing. Boca Raton : Chapman and Hall/CRC, 2019. P. 319–333.

Надійшла до редколегії 16.01.2026
Прийнята до друку після рецензування 23.04.2026
Публікація (оприлюднення) 30.04.2026

Відомості про авторів:

Олексійчук Антон Миколайович – д-р техн. наук, професор, професор спеціальної кафедри № 1 Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Україна; e-mail: alex-dtn@ukr.net; ORCID: https://orcid.org/0000-0003-4385-4631

Покидко Михайло Іванович – директор департаменту цифрової трансформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України, м. Київ; Україна; e-mail: pokydkomi@gmail.com; ORCID: https://orcid.org/0009-0002-9225-5694