УДК 621.391:519.7

С. М. КОНЮШОК, кандидат технічних наук
А М. ОЛЕКСІЙЧУК, доктор технічних наук

БЕЗУМОВНО СТІЙКІ СХЕМИ РОЗПОДІЛУ КЛЮЧІВ В ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ З ВЕЛИКОЮ КІЛЬКІСТЮ АБОНЕНТІВ: II. СХЕМИ БАГАТОАДРЕСНОГО РОЗПОДІЛУ КЛЮЧІВ

Дана стаття є безпосереднім продовженням роботи [1] та містить детальний аналіз відомих методів побудови безумовно стійких схем багатоадресного розподілу ключів (СБРК). Далі в статті вільно використовуються терміни та позначення, що введені в [1].

Серед відомих на сьогодні протоколів розподілу ключів, які дозволяють надійно передавати секретні ключі абонентам відкритими каналами зв'язку та мають криптографічну стійкість, що не залежить від обчислювальних можливостей противника, найбільш перспективними для застосування в інформаційних та телекомунікаційних системах з великою кількістю абонентів вважаються безумовно стійкі схеми багатоадресного розподілу ключів [2 – 7].

Загальновизнаними основоположниками в галузі синтезу СБРК є С. Берковіц [8] та А. Фіат і М. Наор [2], які вперше запропонували використовувати широкомовні канали зв'язку для розподілу секретних ключів групам абонентів, що застосовують певну симетричну криптосистему.

У більшості доступних наукових робіт, які присвячені вирішенню задач побудови або аналізу схем багатоадресного розподілу ключів [2 – 4, 8 – 15], досліджуються властивості так званих "однократних" (one-time) СБРК [3], які забезпечують безумовну стійкість криптографічної процедури вироблення групового ключу лише при однократному застосуванні схеми. Проте, більшість "однократних" схем багатоадресного розподілу ключів може бути перетворена у "багатократні" СБРК з використанням відомих простих алгоритмів [16, 17]. Тому далі термін "схема багатоадресного розподілу ключів" означає саме "однократна" СБРК.

Зауважимо, що на практиці передача сеансових ключів у вигляді "багатоадресних повідомлень" вимагає дотримання певного протоколу, за яким кожний абонент, що належить довільній привілейованій групі P, має однозначно вирішити, яка "частина" цього повідомлення призначена саме йому. Зрозуміло, що така інформація може міститись у повідомленні у відкритому (незашифрованому) вигляді. Проте, це може бути неприйнятним з точки зору забезпечення анонімності абонентів спеціальної телекомунікаційної системи (СТКС). З іншого боку, відомі схеми багатоадресного розподілу ключів, за якими кожний абонент мережі зв'язку повинен знати ідентифікатори інших абонентів відповідних привілейованих груп, оскільки ця інформація застосовується при розшифруванні повідомлень, що передаються з центру розподілу ключів (ЦРК) широкомовним каналом зв'язку [3]. Відмітимо також роботи [9, 11], в яких представлені схеми багатоадресного розподілу ключів, що не вимагають знання абонентами мережі зв'язку ідентифікаторів інших абонентів і, таким чином, дозволяють забезпечити їх анонімність.

1. "Простіші" схеми багатоадресного розподілу ключів

Широко відомі дві "*простіші*" *конструкції схем багатоадресного розподілу ключів* [3, 13]. Перша з них дозволяє будувати СБРК із максимальною багатоадресною інформаційною швидкістю $\rho_M = 1$, виходячи з довільної схеми попереднього розподілу ключів (СПРК) R, такої, що для кожної привілейованої групи P її учасників множина спільних секретних ключів, що обчислюють абоненти з P, є скінченною абелевою групою K, яка не залежить від P (див. [1]). Нехай $l_P \in K$ позначає спільний секретний ключ учасників привілейованої групи P СПРК R. Тоді для передачі з ЦРК секретного групового ключу $k_P \in K$ учасникам цієї групи формується відкрите повідомлення $m_P = k_P + l_P$, яке передається широкомовним каналом зв'язку. Зрозуміло, що побудована таким чином схема багатоадресного розподілу ключів має ту ж саму структуру специфікації, що й вихідна СПРК R. Інформаційна швидкість ρ та повна інформаційна швидкість ρ_T отриманої СБРК дорівнюють відповідно $\rho = \sigma$, $\rho_T = \tau/(\tau+1)$, де σ і τ є відповідно інформаційною швидкістю та повною інформаційною швидкістю вихідної СПРК [3].

Друга "простіша" конструкція СБРК приводить до схем багатоадресного розподілу ключів, що мають максимальну інформаційну швидкість $\rho = 1$. На першому етапі такої СБРК кожному абоненту $i \in V$ з центру розподілу ключів передається секретне значення $u_i \in K$, де K – деяка скінченна абелева група. Далі, на другому етапі груповий ключ $k_P \in K$, що призначається привілейованій групі учасників $P \subseteq V$, перетворюється у відкрите повідомлення $m_P = (u_i + k_P : i \in P)$, яке передається всім абонентам широкомовним каналом зв'язку. Отримана схема багатоадресного розподілу ключів є пороговою $(\le v, v)$-СБРК, має інформаційну швидкість $\rho = 1$, багатоадресну інформаційну швидкість $\rho_M = 1/v$ та повну інформаційну швидкість $\rho_T = 1/(v+1)$, де $v = |V|$ [3].

Конструкції СБРК, що описані вище, ілюструють два крайніх випадки можливого співвідношення між основними показниками ефективності схеми багатоадресного розподілу ключів: її інформаційною швидкістю та багатоадресною інформаційною швидкістю. Як відмічено в [1], зазначені параметри стисло пов'язані між собою та, взагалі кажучи, не можуть бути збільшені одночасно. Отримання певного "компромісу" між інформаційною швидкістю та багатоадресною інформаційною швидкістю СБРК є однією з головних задач сучасних досліджень у галузі безумовно стійких схем розподілу ключів. Відомі способи вирішення цієї задачі приводять до широкого спектру різноманітних СБРК (див. [3, 4, 13, 18]).

2. Класифікація СБРК. Схема Берковиця

В залежності від методів синтезу або конкретних математичних конструкцій, що покладені в основу існуючих СБРК, а також їхніх структур специфікацій, відомі безумовно стійкі схеми багатоадресного розподілу ключів можна умовно поділити на три класи (див. рис. 1 в статті [1]).

До першого класу відносяться СБРК із пороговими структурами специфікацій вигляду $(\le v,\ t)$, де $t \ge 1$. Всі вони (за виключенням "простіших" схем багатоадресного розподілу ключів) будуються на основі так званої "KIO-конструкції" Д. Стінсона або її модифікацій [3, 14, 19]. Іншою загальною ознакою, що об'єднує такі схеми багатоадресного розподілу ключів, є сумісне застосування в їхніх конструкціях певних СПРК з множиною привілейованих груп $\Re = 2^V$ та схем розділення секрету (СРС) [20, 21, 22], зокрема, відомої порогової схеми А. Шаміра [23].

Другий клас складають СБРК, які мають структури специфікацій вигляду $(n,\ t)$, де $n \ge 1$, $t \ge 1$, $n + t \le v$, а також інші (непорогові) схеми багатоадресного розподілу ключів, що будуються з використанням лінійних перетворень та лінійних СПРК [12, 13, 24].

Нарешті, до третього класу можна віднести "комбінаторні" СБРК, які основуються на певних системах підмножин (покриттях) множини абонентів мережі зв'язку [6, 7]. Такі СБРК мають структури специфікацій вигляду $(\ge v - t, t)$, де $t \ge 1$ та (звичайно) є "достатньо малим" або "достатньо великим" числом (див. [7]). За сутністю математичних конструкцій, що лежать в їх основі та визначають їх властивості, зазначені схеми багатоадресного розподілу ключів, в певній мірі, аналогічні схемам попереднього розподілу ключів у розподілених сенсорних мережах [25 – 29] або СПРК типу "KDP" [3, 14, 30 – 33].

Перейдемо до більш детального розгляду методів побудови та аналізу властивостей СБРК, які належать зазначеним вище класам.

Перші конструкції безумовно стійких схем багатоадресного розподілу ключів запропоновані в роботі С. Берковіця [8]. Головна ідея, що покладена в основу таких конструкцій, полягає у використанні порогових схем розділення секрету, що формуються певним чином на етапі широкомовної передачі групового ключу визначеним привілейованим групам учасників СБРК.

Так звана *схема Берковиця* [8] має структуру специфікації $(\le v, v)$ та відноситься до класу "простіших" схем багатоадресного розподілу ключів, які характеризуються інформаційною швидкістю $\rho = 1$ та багатоадресною інформаційною швидкістю $\rho_M = 1/v$ (див. пункт 1).

На першому її етапі кожний абонент $i \in V$ отримує з ЦРК секретну пару цілих чисел $u_i = (x_i, y_i)$, де $x_i \ne 0$, $x_i \ne x_j$ для всіх $i \ne j$ $(i, j \in V)$. Далі, на другому етапі для передачі секретного цілого числа (групового ключу) k_P привілейованій групі $P \subseteq V$ в ЦРК виконують наступні дії.

1. Обирають ціле число $l \ge 0$ та сукупність впорядкованих пар (x_{v+1}, y_{v+1}), (x_{v+2}, y_{v+2}), …, (x_{v+l}, y_{v+l}) цілих чисел таких, що всі значення $x_{v+1}, x_{v+2}, \ldots, x_{v+l}$ є ненульовими, попарно різними та відмінними від $x_1, \ldots, x_v$.

2. Знаходять цілочисельний поліном $f(x)$ степені $n + l$, де $n = |P|$, який задовольняє умовам

(а) $f(0) = k_P$;

(б) $f(x_i) = y_i$ для кожного $i \in P \cup \{v+1, v+2, \ldots, v+l\}$;

(в) $f(x_i) \neq y_i$ для кожного $i \in V \setminus P$.

3. Обирають $n + l$ різних ненульових цілих чисел z_j ($j \in \overline{1, n+l}$) таких, що $z_j \notin \{x_i : i \in \overline{1, v+l}\}$ для кожного $j \in \overline{1, n+l}$, та передають широкомовним каналом зв'язку складене повідомлення $m_P = ((z_j, f(z_j)) : j \in \overline{1, n+l})$ всім абонентам мережі.

Зрозуміло, що внаслідок умови 2(б), кожний абонент $i \in P$ здатний однозначно відновити коефіцієнти поліному $f(x)$ степені $n + l$ за його значеннями в $n + l + 1$ різних точках z_j, $j \in \overline{1, n+l}$ та x_i (наприклад, використовуючи інтерполяційну формулу Лагранжа [30, 34]). Отже, кожний такий абонент має отримати значення k_P, виходячи з умови 2(а). При цьому, внаслідок умови 2(в), всі абоненти, що не належать привілейованій групі *P*, не зможуть встановити секретний ключ k_P, навіть, якщо вони об'єднають власні секретні значення, які отримані ними на першому етапі.

Як видно з приведеного вище опису, СБРК Берковиця основується на тому ж самому принципі, що й порогова СРС А. Шаміра (див., наприклад, [22, 30]).

Зауважимо також, що конкретне значення параметру $l \geq 0$ не впливає на (безумовну) стійкість розглянутої схеми багатоадресного розподілу ключів. Воно дозволяє "маскувати" число абонентів, які належать певній привілейованій групі, та не повинне бути надто великим [35].

3. Схеми Фіата – Наора

Інший підхід до вирішення задачі побудови СБРК запропонований в роботі А. Фіата і М. Наора [2], де подано декілька конструкцій як обчислювально стійких, так і безумовно стійких схем розподілу ключів. Одним з основних результатів [2] є загальний метод побудови $(\leq v, t)$-СБРК, виходячи з довільної $(\leq v, 1)$-СПРК, на основі так званих досконалих сімей геш-функцій.

Згідно [36], система $F = (f_h : h \in \overline{1, l})$ відображень множини $V = \{1, 2, \ldots, v\}$ у множину $\{1, 2, \ldots, m\}$, де $1 \leq m < v$, називається *досконалою сім'єю геш-функцій* (або *досконалою геш-сім'єю*) *з параметрами* (l; v, m, t), якщо для довільної t-підмножини $C \subseteq V$ існує таке $h \in \overline{1, l}$, що обмеження функції f_h на множину C є взаємно однозначним відображенням.

Нехай задані $(\leq v, 1)$-СПРК *R* та досконала геш-сім'я *F* з параметрами (l; v, m, t). *Схема Фіата – Наора багатоадресного розподілу ключів*, що основується на даних *R* та *F* [2], будується з використанням матриці $\|R(h, a)\|$ розміру $l \times m$, елементи якої є копіями СПРК *R*, що застосовуються далі незалежно одна від одної.

Перший етап цієї СБРК полягає в передачі з ЦРК кожному абоненту $i \in V$ l наборів секретних ключів, які розподіляються з використанням l СПРК $R(h, f_h(i))$, $h \in \overline{1, l}$, відповідно. Слід відмітити, що при цьому в силу досконалості геш-сім'ї *F* для кожної множини $C \subseteq V$ потужності t існує таке

значення h, що будь-які абоненти i_1, $i_2 \in C$ ($i_1 \neq i_2$) отримують набори секретних ключів за різними СПРК $R(h, f_h(i_1))$ та $R(h, f_h(i_2))$ відповідно.

На другому етапі СБРК Фіата – Наора здійснюється передача з ЦРК довільній привілейованій групі $P \subseteq V$ секретного групового ключу k_P, який являє собою випадкову та рівноймовірну двійкову послідовність довжиною N. Для цього генеруються незалежні у сукупності випадкові та рівноймовірні двійкові послідовності $k(h)$, $h \in \overline{1,l}$, кожна з яких має довжину N, та обчислюється повідомлення

$$k(l) = k_P \oplus k(1) \oplus \ldots \oplus k(l-1).$$

Далі для кожних $h \in \overline{1,l}$, $a \in \overline{1,m}$ центр розподілу ключів застосовує СПРК $R(h,a)$ для широкомовної передачі повідомлення $k(h)$ групі абонентів $P(h,a) = \{i \in V: f_h(i) = a\}$. (Іншими словами, СПРК $R(h,a)$ використовується як "простіша" схема багатоадресного розподілу ключів (див. пункт 1), за якою повідомлення $k(h)$ зашифровується на спільному ключі учасників групи $P(h,a)$, й отримане шифроване повідомлення передається широкомовним каналом зв'язку всім абонентам мережі).

Оскільки для будь-яких $i \in P$, $h \in \overline{1,l}$ існує $a \in \overline{1,m}$ таке, що $i \in P(h,a)$, то кожний учасник групи P здатний отримати всі повідомлення $k(h)$, $h \in \overline{1,l}$ та обчислити за ними ключ k_P. Проте, внаслідок відміченої вище властивості геш-сім'ї F, для будь-якої коаліції C, що складається не більше, ніж з t учасників, існує, щонайменше, одне повідомлення $k(h)$, яке залишається цієї коаліції невідомим.

Таким чином, отримана схема багатоадресного розподілу ключів є t-стійкою та має структуру специфікації $(\leq v, t)$. Згідно [2], її інформаційна швидкість та багатоадресна інформаційна швидкість дорівнюють відповідно $\rho = (lw)^{-1}$ та $\rho_M = (lm)^{-1}$, де w – кількість секретних ключів, що отримує з ЦРК кожний абонент за схемою попереднього розподілу ключів R. Зокрема, якщо в якості СПРК R використовується 1-стійка схема Фіата – Наора, то $w = v$ (див. першу рівність (3) з [1]), і відповідна СБРК Фіата – Наора має інформаційну швидкість $\rho = (vl)^{-1}$, багатоадресну інформаційну швидкість $\rho_M = (ml)^{-1}$ та повну інформаційну швидкість $\rho_T = (v+m+1)^{-1} l^{-1}$ [3].

Отже, в будь-якому випадку метод Фіата – Наора дозволяє отримати ефективну (за інформаційною швидкістю або багатоадресною інформаційною швидкістю) СБРК лише за умовами існування досконалих $(l; v, m, t)$-геш-сімей з малим значенням параметру l (або параметру m) та "високошвидкісних" 1-стійких СПРК, що характеризуються малими значеннями параметру w.

Зауважимо, що, внаслідок оптимальності СПРК Фіата – Наора (див. [1], пункт 3), значення w не може бути менше, ніж v. З іншого боку, згідно [3], існуючі методи побудови досконалих геш-сімей, що мають малі потужності l, є занадто складними, а існування більшості "якісних" геш-сімей (з достатньо малими l) встановлено лише з використанням неконструктивних, імовірнісних, міркувань.

Отже, в цілому, існують певні обмеження щодо суттєвого збільшення значень інформаційних швидкостей або забезпечення потрібного, з практичної точки зору, співвідношення між характеристиками схем багатоадресного розподілу ключів, які будуються за методом Фіата – Наора. Це обумовлено як відсутністю на сьогоднішній день простих конструктивних методів синтезу досконалих геш-сімей малої потужності, так і власно слабкими обмеженнями щодо структур специфікацій СБРК, які основуються на зазначених геш-сім'ях (а саме, за визначенням будь-яка група учасників такої СБРК утворює привілейовану коаліцію).

З метою подолання відмічених недоліків, в [2] запропоновано використовувати для побудови СБРК дві обчислювально 1-стійкі СПРК, що характеризуються значеннями параметру $w = \log v$ та $w = 1$ відповідно. Проте перша з цих схем попереднього розподілу ключів є стійкою лише за умовою існування важкооборотних функцій (питання про справжність цього твердження складає одну з невирішених складних проблем сучасної криптографії [37]). Друга СПРК еквівалентна за стійкістю криптосистемі RSA (обчислювальна стійкість якої основується на недоведеній гіпотезі про складність задачі цілочисельної факторизації [35]).

Остання схема попереднього розподілу ключів складається з наступних двох етапів. На першому етапі ЦРК обирає два секретні прості числа та публікує їх добуток N. Далі, він обирає секретне ціле число $g < N$, що має великий мультиплікативний порядок за модулем N. Кожен абонент $i \in V$ отримує з ЦРК секретний ключ $u_i = g^{p_i} \pmod N$, де p_i, $i \in V$ – попарно взаємно прості числа, які відомі всім учасникам СПРК. На другому етапі учасники довільної привілейованої групи $P \subseteq V$ обчислюють спільний секретний ключ $k_P = g^{\prod_{i \in P} p_i} \pmod N$, при цьому *i*-й учасник ($i \in V$) отримує k_P шляхом піднесення власного секретного ключа $u_i = g^{p_i}$ до степені $\prod_{r \in P - \{i\}} p_r$ за модулем N.

В [2] показано, що за припущенням щодо великої обчислювальної складності задачі розв'язання квадратних рівнянь у кільці лишків за модулем великого складеного числа (яка еквівалентна за складністю задачі цілочисельної факторизації [35, 38]), описана СПРК є обчислювально 1-стійкою. Слід також зауважити, що дана схема розподілу ключів не є 2-стійкою, оскільки елемент g можливо легко знайти за формулою $g = k^{a_1} k^{a_2}$, де цілі числа a_1, a_2 задовольняють рівності $a_1 p_1 + a_2 p_2 = 1$ і можуть бути отримані з використанням алгоритму Евкліда.

Одним з головних результатів, що отримані в [2], є теорема про існування t-стійкої схеми багатоадресного розподілу ключів, за якою число n_t секретних ключів, що отримує з ЦРК кожний абонент мережі зв'язку, та число χ_t зашифрувань, які виконуються в ЦРК на етапі передачі групового ключу довільній привілейованій групі учасників, дорівнюють відповідно

$$n_t = O(t \log t \log v),\ \chi_t = O(t^2 (\log t)^2 \log v),\ v, t \to \infty.$$

Така СБРК будується за модифікацією викладеного вище методу на основі обчислювально 1-стійкої СПРК та двох досконалих геш-сімей, існування яких встановлюється, виходячи з імовірнісних міркувань. Проте зазначена СБРК має лише обчислювальну стійкість.

4. Метод Д. Стінсона побудови СБРК

Головна ідея, що покладена в основу методу Фіата – Наора, розвинута та узагальнена в [3], де запропонована так звана "KIO-конструкція" побудови безумовно стійких схем багатоадресного розподілу ключів. Її сутність полягає у сумісному застосуванні для отримання СБРК зі структурою специфікації вигляду $(\le v,\ \Im)$, де $\Im \subseteq 2^V$, безумовно стійких СПРК Фіата – Наора та певної ідеальної схеми розділення секрету над скінченним полем.

Вихідними даними для "*KIO-конструкції*" *Стінсона* [3] є сукупність $\widetilde{B} = \{B_1, \ldots, B_\beta\}$ підмножин множини V, натуральне число θ, клас множин $\Im \subseteq 2^V$ та ідеальна схема розділення секрету над полем із q елементів, яка реалізує структуру доступу $\Gamma \subseteq 2^{\widetilde{B}}$ [20]. При цьому потрібне виконання таких умов:

(а) $\{B_j \in \widetilde{B} : i \in B_j\} \in \Gamma$ для кожного $i \in V$;

(б) $\{B_j \in \widetilde{B} : \left|C \cap B_j\right| \ge \theta + 1\} \notin \Gamma$ для кожного $C \in \Im$.

Згідно [3], за визначеними даними можна створити $(\le v, \Im)$-СБРК, що складається з двох наступних етапів.

На першому етапі для кожного $j \in \overline{1,\beta}$ на множині учасників B_j будується $(\le \left|B_j\right|, \theta)$-СПРК Фіата – Наора (див. [1], пункт 3), за якою для кожної множини $C \subseteq B_j$, де $\left|C\right| \le \theta$, в центрі розподілу ключів генерується секретний ключ $s_{jC} \in$ **GF**(q), що передається захищеним каналом зв'язку кожному абоненту з множини $B_j \setminus C$. Підкреслимо, що генерація ключів у зазначених СПРК здійснюється за незалежною схемою без повернення (тобто усі елементи s_{jC} є незалежними у сукупності та рівноймовірними випадковими величинами, що розподілені на **GF**(q)).

На другому етапі для передачі довільній привілейованій групі учасників $P \subseteq V$ секретного групового ключу $k_P \in$ **GF**(q) використовується такий алгоритм.

1. Для кожного $j \in \overline{1,\beta}$ ЦРК знаходить j-ту проекцію $y_j \in$ **GF**(q) секретного ключу k_P.

2. Для кожного $j \in \overline{1,\beta}$ ЦРК обчислює ключ k_j, що відповідає підмножині $P \cap B_j$ у визначеній вище СПРК Фіата-Наора на множині учасників B_j,

$$k_j = \sum_{\{C \subseteq B_j : C \cap P = \varnothing, |C| \le \theta\}} s_{jC} .$$

3. Для кожного $j \in \overline{1,\beta}$ ЦРК знаходить повідомлення $m_j = y_j + k_j$, формує складене повідомлення $m_P = (m_j : j \in \overline{1,\beta})$ та передає його широкомовним каналом зв'язку всім абонентам мережі.

В [3] показано, що, внаслідок умов (а), (б), кожний абонент $i \in P$ здатний відновити ключ k_P за отриманим повідомленням m_P; при цьому будь-яка заборонена коаліція $C \in \Im$ $(C \cap P = \varnothing)$ не отримує жодної інформації про k_P.

В [3, 14] приведені численні приклади застосування "КІО-конструкції" для побудови СБРК на основі різноманітних комбінаторних конфігурацій (неповних урівноважених блок-схем (НУБС), ортогональних таблиць, систем Штейнера, універсальних геш-сімей) та порогових СРС Шаміра. Також показано, що СБРК Фіата – Наора являє собою частинний випадок схеми багатоадресного розподілу ключів, що основується на "КІО-конструкції" Стінсона. Найбільш ефективні СБРК, що отримані з використанням "КІО-конструкції" в [3, 14, 19], є схеми багатоадресного розподілу ключів, які основуються на так званих (v, b, r, λ)-конфігураціях. Останні є безпосереднім узагальненням неповних урівноважених блок-схем [39] та визначаються наступним чином [14].

Впорядкована пара $D = (V, \widetilde{B})$, де V – скінченна множина потужності v, а $\widetilde{B} = \{B_1, \ldots, B_b\}$ – сукупність підмножин (блоків) множини V, що має потужність b, називається (v, b, r, λ)-*конфігурацією*, якщо кожен елемент $i \in V$ належить точно r блокам B_j, $j \in \overline{1,b}$, а кожна пара різних елементів $i, j \in V$ належить не більше ніж λ блокам B_j, $j \in \overline{1,b}$.

Якщо кожна пара різних елементів $i, j \in V$ належить точно λ блокам B_j, $j \in \overline{1,b}$, та всі блоки (v, b, r, λ)-конфігурації D мають рівну потужність $k < v - 1$, то D являє собою *неповну урівноважену блок-схему* або (b, v, r, k, λ)-*конфігурацію*. Відомо [39], що параметри b, v, r, k, λ будь-якої НУБС задовольняють співвідношенням

$$vr = bk, \ \lambda(v-1) = r(k-1), \ v \le b. \qquad (1)$$

У випадку $v = b$ (або, що рівносильно, $k = r$) (b, v, r, k, λ)-конфігурація D називається *симетричною блок-схемою* або (v, k, λ)-*конфігурацією*. Відмітимо, що на сьогоднішній день симетричні (та деякі інші) НУБС складають один з найбільш вивчених класів комбінаторних конфігурацій. Викладенню їх загальної теорії присвячені монографії [39, 40].

В статті [14] представлена схема багатоадресного розподілу ключів із структурою специфікації $(\le v, t)$, що основується на довільній (v, b, r, λ)-конфігурації D, параметри якої задовольняють умові

$$r > \lambda \binom{t}{2}. \qquad (2)$$

Зазначена СБРК будується на основі "КІО-конструкції" з використанням порогової СРС Шаміра та має інформаційну швидкість ρ і багатоадресну інформаційну швидкість ρ_M, які дорівнюють відповідно

$$\rho = (r + \lambda(v-1))^{-1},\ \rho_M = b^{-1}. \quad (3)$$

В [19] запропонована модифікація методу з [14], що використовує для побудови СБРК замість порогових СРС так звані "*рамп-схеми*" з параметрами (c, r, b), $1 \le c < r \le b$ (тобто схеми розділення секрету на множині з b учасників, за якими кожна група учасників, що має потужність не менше ніж r, цілком відновлює секретний ключ, а кожна група учасників потужності не більше c не отримує про нього жодної інформації).

Нехай задані (v, b, r, λ)-конфігурація $D = (V, \widetilde{B})$ та натуральне число t. Згідно визначенню [14], конфігурація D називається *t-пороговою*, якщо для кожного $F \subseteq V$, $|F| \le t$ виконується нерівність

$$c_F \overset{\text{def}}{=} |\{B \in \widetilde{B} : |F \cap B| \ge 2\}| \le r-1.$$

В [19] показано, що для кожної t-порогової (v, b, r, λ)-конфігурації D, яка задовольняє умові $1 \le c \overset{\text{def}}{=} \max\{c_F: F \subseteq V, |F| \le t\} < r$, можна побудувати $(\le v, t)$-СБРК, що має інформаційну швидкість ρ та багатоадресну інформаційну швидкість ρ_M, які перевищують відповідні значення (3) не менше, ніж у $r - c$ разів:

$$\rho \ge (r-c)(r + \lambda(v-1))^{-1},\ \rho_M = (r-c)b^{-1}. \quad (4)$$

Зокрема, один із головних результатів статті [19] встановлює, що для довільного примарного q та натурального $k \le q$ за виконанням умов

$$v \le q^k,\ t(t-1) < 2q(k-1)^{-1} \quad (5)$$

існує $(\le v, t)$-СБРК зі швидкостями

$$\rho \ge \frac{q - \binom{t}{2}(k-1)}{q + (k-1)(v-1)},\ \rho_M \ge \frac{q - \binom{t}{2}(k-1)}{q^2}. \quad (6)$$

Схеми багатоадресного розподілу ключів, що мають значення швидкостей вигляду (4) або (6), утворюють найбільш ефективний (з відомих авторам даної статті) класів $(\le v, t)$-СБРК, які будуються з використанням "КІО-конструкції" Стінсона [3]. Проте ряд суттєвих недоліків, що притаманні СБРК Фіата – Наора (яка також належить до цього класу), наслідуються усіма зазначеними схемами розподілу ключів. По-перше, це – занадто малі значення інформаційної швидкості ρ (як витікає з [19], кожен абонент СБРК, що розглядається, повинен зберігати не менше секретних ключів, ніж загальна кількість v абонентів мережі зв'язку). По-друге, слабкі обмеження щодо структур специфікацій зазначених СБРК (кожна підмножина множини V є привілейованою коаліцією) взагалі роблять проблематичним суттєве збільшення ефективності (за інформаційною або багатоадресною інформаційною швидкістю) відомих $(\le v, t)$-СБРК. Також, за виключенням певних окремих випадків (наприклад, $t = 2$), умови існування (v, b, r, λ)-конфігурацій з малими значеннями b [14] об'єктивно обмежують ефективність $(\le v, t)$-СБРК, що відповідають таким конфігураціям. Нарешті, в силу нерівності (2) та другої нерівності (5) відповідні t-стійкі СБРК можуть

бути побудовані з використанням "КІО-конструкції" тільки за достатньо малими значеннями t (порядку $\sqrt{2r\lambda^{-1}}$ та $\sqrt{2q(k-1)^{-1}}$ відповідно).

5. Лінійні схеми багатоадресного розподілу ключів

Як відмічено вище, метою створення будь-якої схеми багатоадресного розподілу ключів із заданою структурою специфікації є підвищення інформаційної швидкості СПРК, що має таку структуру, за рахунок певного зменшення багатоадресної інформаційної швидкості "простішої" СБРК, яка відповідає зазначеній схемі попереднього розподілу ключів. Складність вирішення цієї задачі визначається саме типом структури специфікації, для якої потрібно сконструювати безумовно стійку схему багатоадресного розподілу ключів, що забезпечує необхідний "баланс" між значеннями інформаційної та багатоадресної інформаційної швидкостей. На сьогоднішній день загальні конструктивні методи синтезу СБРК, що задовольняють зазначеній умові, відомі лише для структур специфікацій вигляду (n, t), де $n \ge 1$, $t \ge 1$, $n + t \le v$ [12], та ряду інших (непорогових) структур специфікацій, що визначаються декілька складніше [13].

Найбільш загальний метод побудови СБРК зазначеного типу запропонований в [13]. Його сутність полягає у побудові для кожної привілейованої групи P її певного покриття підмножинами множини V, визначенні на цій множині нової структури специфікації, що може бути реалізована з використанням деякої лінійної схеми попереднього розподілу ключів [24], та отриманні відповідним чином на основі такої СПРК і певних лінійних перетворень схеми багатоадресного розподілу ключів.

Основний результат статті [13] можливо сформулювати наступним чином. Нехай Г – задана структура специфікації на множині V, $\Re$ – сукупність всіх Г-привілейованих множин (див. [1], пункт 2). Нехай, далі, для кожного $P \in \Re$ задана деяка сукупність B_P підмножин множини V, що задовольняють умовам $Q \not\subset Q'$ для будь-яких різних $Q, Q' \in B_P$; $\bigcup_{Q \in B_P} Q = P$.

Покладемо $B = \{ B_P \colon P \in \Re \}$ та визначимо на множині V нову структуру специфікації

$$\Gamma_B = \{(Q, F') \in 2^V \times 2^V \mid \exists (P, F) \in \Gamma : Q \in B_P, F' = F \cup (P \setminus Q)\}. \qquad (7)$$

Припустимо, що існує лінійна Γ_B-СПРК R, яка має інформаційну швидкість τ. В цьому випадку існує Г-СБРК $\widetilde{R}$, що має інформаційну швидкість $\rho = \mu\tau$ та багатоадресну інформаційну швидкість $\rho_M = \mu M^{-1}$, де

$$\mu = \min_{P \in \Re, i \in P} \{| Q \in B_P : i \in Q |\}, \; M = \max\{| B_P | : P \in \Re\}. \qquad (8)$$

Зазначена СБРК може бути побудована з використанням конкретного алгоритму, що викладений в [13].

Підкреслимо, що в якості лінійної СПРК R, в принципі, може бути обрана будь-яка з відомих порогових схем попереднього розподілу ключів (тривіальна схема, СПРК Фіата – Наора або "схема Бландо та інших"; див. [1]), оскільки всі зазначені СПРК є лінійними схемами [24]. Разом з тим, слід відзначити, що у багатьох важливих випадках (наприклад, для структур специфікацій Г =

$(\le n,\ t)$, де $n \ge 1,\ t \ge 1$) метод із [13] поки що не дозволяє отримувати схеми багатоадресного розподілу ключів із зазначеними вище швидкостями, внаслідок складності будови відповідних структур специфікацій Γ_B вигляду (7).

На сьогодні, ймовірно, єдиним відомим прикладом СБРК, що мають порогові структури специфікацій та можуть бути отримані з використанням конструкції з [13], є схеми багатоадресного розподілу ключів, які запропоновані раніше К. Бландо, Л. Фрото-Маттосом та Д. Стінсоном [12].

Нехай задані натуральні числа n та t, де $n+t \le v$. Тоді для кожного $l \in \overline{1, n}$ існує схема багатоадресного розподілу ключів $\widetilde{R} = \widetilde{R}_l$, що має структуру специфікації $\Gamma = (n,\ t)$, інформаційну швидкість ρ, багатоадресну інформаційну швидкість ρ_M та повну інформаційну швидкість ρ_T, які дорівнюють відповідно [12]

$$\rho = \binom{n-1}{l-1}\binom{n+t-1}{l-1}^{-1},\ \rho_M = ln^{-1},\ \rho_T = \binom{n-1}{l-1}\left(\binom{n+t}{l}+\binom{n-1}{l-1}\right)^{-1}. \qquad (9)$$

Як показано в [13], зазначену БСРК $\widetilde{R}_l$ можливо побудувати, виходячи з сукупностей множин $\Re = \{P \in 2^V: |P| = n\}$ та $B = \{B_P: P \in \Re\}$, де $B_P = \{Q \in 2^P: |Q| = l\}$ для кожного $P \in \Re$. Згідно рівності (7), в цьому випадку структура специфікації Γ_B має вигляд $(l,\ n+t-l)$. Отже, в якості лінійної Γ_B-СПРК R можна використовувати "схему Бландо та інших" [41], інформаційна стійкість якої дорівнює $\tau = \binom{n+t-1}{l-1}$ (див. [1], пункт 3). Виходячи з формул (8) та визначення множин $B_P,\ P \in \Re$, неважно впевнитись в тому, що $\mu = \binom{n-1}{l-1}$, $M = \binom{n}{l}$. Таким чином, в силу приведеного вище результату [13], існує $(n,\ t)$-СБРК $\widetilde{R}_l$, параметри $\rho = \mu\tau$ та $\rho_M = \mu M^{-1}$ якої визначаються за першими двома формулами (9).

Відмітимо, що оригінальні конструкції [12] схем багатоадресного розподілу ключів із параметрами вигляду (9) певно відрізняються від їх "лінійного узагальнення" з [13].

Важлива перевага методу побудови СБРК, що запропонований в [12], полягає в можливості забезпечення достатньо гнучкого "балансу" між характеристиками ефективності схем багатоадресного розподілу ключів шляхом вибору відповідних значень параметру l. Так, максимальну інформаційну швидкість $\rho = 1$ СБРК $\widetilde{R}_l$ можливо отримати, прийнявши $l = 1$ (при цьому $\widetilde{R}_l$ зводиться до однієї з "простіших" СБРК, що розглянуті в пункті 1). З іншого боку, якщо необхідно максимізувати значення багатоадресної інформаційної швидкості СБРК $\widetilde{R}_l$ (тобто отримати $\rho_M = 1$), достатньо покласти $l = n$ (див. рівності (9)). Пошук найбільш прийнятного, за тих чи

інших умов, співвідношення між значеннями обох швидкостей СБРК здійснюється шляхом вибору значень параметру l у вказаних межах.

Як відмічено в [13], задача побудови лінійних схем багатоадресного розподілу ключів, що мають більш прийнятні, з практичної точки зору, порогові структури специфікацій (вигляду $(\le n,\ t)$, де $n \ge 1$, $t \ge 1$, $n+t \le v$, або $(\ge v-t,\ t)$, де $1 \le t < v$) залишається на сьогодні невирішеною. Також відкрито питання про оптимальність СБРК із параметрами ρ, ρ_M вигляду (9) [13, 18].

6. Схеми багатоадресного розподілу ключів, що основуються на покриттях множини абонентів

В роботах [6, 7] запропонований загальний підхід до синтезу схем багатоадресного розподілу ключів, який певно відрізняється від розглянутих вище методів їх побудови. Сутність відмін полягає як у математичних конструкціях і методах, що використовуються при побудові та дослідженні ефективності зазначених СБРК, так і в застосуванні декілька інших показників ефективності таких схем розподілу ключів. Згодом даний підхід (під назвою "subset-cover framework" [42]) отримав значний розвиток в [42, 43, 44] і ряді інших робіт, де на його основі запропоновані та досліджені (головним чином, умовно стійкі) ефективні СБРК. Відмітимо також статті [25 – 29, 45], які присвячені аналізу властивостей схем попереднього розподілу ключів, що будуються на основі систем скінченних множин.

Нижче приведений стислий огляд понять та результатів [6, 7], які встановлюють властивості безумовно стійких СБРК, що основуються на покриттях множини абонентів мережі зв'язку.

Нехай V – скінченна множина потужності v, $\widetilde{B}$ – сукупність b різних підмножин (блоків) множини V. Впорядкована пара $D = (V, \widetilde{B})$ називається *системою множин*. При цьому говорять, що сукупність $\widetilde{B}$ утворює *покриття* множини V (або що множини $B \in \widetilde{B}$ *покривають* V), якщо виконується умова [46]

$$\bigcup \{B : B \in \widetilde{B}\} = V. \qquad (10)$$

Кожній системі множин $D = (V, \widetilde{B})$, що задовольняє рівності (10), можна поставити у відповідність схему багатоадресного розподілу ключів на множині учасників V, яка визначається наступним чином [6].

На першому етапі в ЦРК генерують b випадкових, незалежних у сукупності секретних ключів u_B, де $B \in \widetilde{B}$, що мають рівномірні розподіли ймовірностей на деякій скінченній абелевій групі K. Далі кожному абоненту $i \in V$ із центру розподілу ключів передаються захищеним каналом зв'язку всі ключі u_B такі, що $i \in B$, де $B \in \widetilde{B}$.

Нехай $P \subseteq V$ є фіксованою привілейованою групою абонентів, $C = V \setminus P$. На другому етапі для передачі секретного групового ключу $k_P \in K$ учасникам групи P в ЦРК формується так звана *залишкова* (*відносно множини* C) *конфігурація*, тобто система множин $D_P = (P, \widetilde{B}_P)$, де $\widetilde{B}_P = \{B \in \widetilde{B} : B \subseteq P\}$ [6]. Якщо сукупність $\widetilde{B}_P$ є покриттям множини P, тобто

$$\bigcup \{B : B \in \widetilde{B}_P\} = P, \tag{11}$$

то в центрі розподілу ключів з використанням заздалегідь визначеного алгоритму отримують деяку сукупність різних блоків $B_1, \ldots, B_s \in \widetilde{B}_P$ ($s \in \boldsymbol{N}$), що покривають множину P, та формують складене повідомлення

$$m_P = (k_P + u_{B_i} : i \in \overline{1, s}), \tag{12}$$

яке передається широкомовним каналом зв'язку всім абонентам мережі.

Зрозуміло, що виконання рівності (11) є необхідною умовою, за якою довільна множина $P \subseteq V$ складає привілейовану групу учасників визначеної СБРК. При цьому, як витікає з рівності (12) й умови незалежності та рівноймовірності секретних ключів u_B, $B \in \widetilde{B}$, кожний абонент $i \in C$ не отримує жодної інформації про груповий ключ k_P.

Далі схему багатоадресного розподілу ключів, яка відповідає системі множин $D = (V, \widetilde{B})$, що задовольняє умові (10), будемо позначати таким самим символом D. Множини $B \in \widetilde{B}$ іноді будемо називати *локальними ключовими мережами* (ЛКМ) схеми багатоадресного розподілу ключів, що основується на системі множин D [45].

У відповідності з визначенням [2] СБРК D є t-стійкою, якщо для кожної множини $P \subseteq V$ потужності $|P| \geq v - t$ виконується рівність (11). Найбільше невід'ємне ціле число t, для якого D є t-стійкою схемою розподілу ключів, називається *стійкістю СБРК* D [6] та позначається символом $\tau(D)$.

Отже, в якості структури специфікації СБРК D зі стійкістю $\tau(D) = t$, можливо обрати сукупність множин $\Gamma = \{(P, C) \in 2^V \times 2^V : |C| \leq t, P = V \setminus C\}$, тобто, згідно позначенням із [1], $\Gamma = (\geq v - t, t)$.

Для кількісної оцінки ефективності СБРК, що основуються на покриттях множини абонентів, як правило, використовують числові параметри, які вважаються більш адекватними, з практичної точки зору, ніж показники ρ та ρ_M [6, 7]. Зауважимо, що вперше такі параметри запропоновані ще А. Фіатом та М. Наором [2], в якості основних характеристик ефективності довільних СБРК. Вони використовуються також у [42 – 44, 47, 48] при аналізі властивостей ряду обчислювально стійких схем багатоадресного розподілу ключів.

Згідно [2, 6, 7], *основними показниками ефективності СБРК* $D_P = (P, \widetilde{B}_P)$ є

(1) максимальне число $n(D)$ секретних ключів u_B ($B \in \widetilde{B}$), що отримує з ЦРК кожний абонент мережі зв'язку на першому етапі:

$$n(D) = \max_{i \in V} |\{B \in \widetilde{B} : i \in B\}|;$$

(2) максимальна довжина s повідомлень вигляду (12), що формуються на другому етапі для передачі секретного групового ключу k_P довільній привілейованій групі $P \subseteq V$ потужності $v - t$, $t \in \overline{0, \tau(D)}$.

Остання характеристика має назву *t-зв'язності СБРК* D [6] та позначається далі символом $\chi_t(D)$.

Відзначимо, що t-зв'язність даної СБРК D є функцією цілочисельного параметру $t \in \overline{0, \tau(D)}$, яка залежить від конкретного алгоритму побудови

покриття довільної множини $P \subseteq V$ потужності $v - t$ блоками залишкової конфігурації D_P (див. рівності (11), (12)). Як правило, вважається, що таким покриттям є будь-яке *мінімальне* (за кількістю блоків) *покриття* множини P [6, 7]. Отже, далі, якщо не зосереджено супротивне, вважатимемо, що t-зв'язність СБРК D співпадає з максимумом складностей мінімальних покрить привілейованих груп абонентів, що мають потужність $v - t$, блоками відповідних залишкових конфігурацій, $t \in \overline{0, \tau(D)}$.

В якості *додаткового показника ефективності СБРК* $D = (V, \widetilde{B})$ можна вважати загальну кількість b секретних ключів, що генеруються в ЦРК на першому етапі даної схеми розподілу ключів. Підкреслимо, що порівняння ефективності (за визначеними вище показниками) будь-яких СБРК $D = (V, \widetilde{B})$ та $D' = (V', \widetilde{B}')$ є коректним лише за умовою рівності їхніх структур специфікацій, тобто у випадку, коли $|V| = |V'|$, $\tau(D) = \tau(D')$.

Неважко отримати вирази швидкостей довільної СБРК D, що основується на покритті множини абонентів, через визначені вище параметри $n(D)$, $\chi_t(D)$, $t \in \overline{0, \tau(D)}$. Дійсно, як випливає з умови незалежності та рівноймовірності секретних ключів u_B, $B \in \widetilde{B}$, що розподіляються між абонентами на першому етапі СБРК D, її інформаційна швидкість та багатоадресна інформаційна швидкість дорівнюють відповідно

$$\rho = n(D)^{-1},\ \rho_M = (\max\{\chi_t(D):\ t \in \overline{0, \tau(D)}\})^{-1}.$$

В зв'язку з аналізом ефективності (за зв'язністю або максимальним числом секретних ключів учасників) схем багатоадресного розподілу ключів, що основуються на покриттях множини абонентів, в [7] і [42] отримані нижні границі параметрів $n(D)$ та, відповідно, $\chi_1(D)$ довільної 1-стійкої СБРК $D = (V, \widetilde{B})$.

Результати [7, 42] основуються на так званій лемі про соняшник, яка доведена в [49]. За визначенням *соняшником* називають довільну систему множин $(U, \widetilde{F})$, де $\widetilde{F} = \{F_1, \ldots, F_M\}$, яка задовольняє умові

$$F_i \cap F_j = \bigcap_{\nu=1}^{M} F_\nu,\ 1 \le i < j \le M.$$

Лема про соняшник [49] стверджує, що кожна система з L непустих різних підмножин $G_1, \ldots, G_L$ скінченної множини U така, що $|G_i| \le m$, $i \in \overline{1, L}$, містить, в якості підсистеми, соняшник $(U, \widetilde{F})$ потужності $|\widetilde{F}| \ge m^{-1} L^{1/m}$.

З використанням цієї леми в [7] отримана нижня оцінка параметру $n(D)$ 1-стійкої СБРК D, а саме, показано, що для будь-якого $t \in \overline{1, \tau(D)}$

$$n(D) \ge (t\chi_t)^{-1} \left(\binom{v}{t}^{1/\chi_t} - \chi_t \right), \qquad (13)$$

де $\chi_t = \chi_t(D)$ – t-зв'язність СБРК D. Аналогічна за сутністю оцінка параметру $\chi_1(D)$ (1-зв'язності СБРК D) встановлена в [42]:

$$\chi_1(D) \geq n^{-1}\left(v^{1/n} - n\right), \tag{14}$$

де $n = n(D)$ – максимальне число секретних ключів, що зберігає кожний учасник СБРК D.

Обидві нерівності доводяться простим застосуванням леми про соняшник до відповідних систем множин. Для доведення оцінки (13) (див. [7]) позначимо символом G_P (де $P \subseteq V$, $|P| = v - t$) множину всіх секретних ключів u_B, $B \in \widetilde{B}$, що використовуються в ЦРК для формування складеного повідомлення m_P вигляду (12), яке призначається даній привілейованій групі P учасників СБРК $D = (V, \widetilde{B})$. За визначенням t-зв'язності СБРК D для кожного $P \subseteq V$, де $|P| = v - t$, виконується нерівність $|G_P| \leq \chi_t$. Отже, згідно лемі про соняшник, існує не менше ніж

$$M = \chi_t^{-1}\binom{v}{t}^{1/\chi_t}$$

множин $G_{P(1)}, \ldots, G_{P(M)}$ із сукупності $\{G_P: P \subseteq V, |P| = v - t\}$, що утворюють соняшник. Нехай $C = V \setminus P(1)$ є забороненою відносно $P(1)$ коаліцією учасників СБРК D, K_C – об'єднання множин секретних ключів абонентів коаліції C. З визначення соняшнику випливає, що існують попарно різні ключі $u_2, \ldots, u_M$ такі, що $u_i \in K_C \cap G_{P(i)}$, $i \in \overline{2, M}$. Таким чином, $|K_C| \geq M - 1$ й, оскільки $|C| = t$, то існує, що найменш, один учасник коаліції C, який зберігає не менше, ніж $t^{-1}(M - 1)$ секретних ключів. Отже, $n(D) \geq t^{-1}(M - 1)$, що і треба було довести.

Аналогічно, застосовуючи лему про соняшник до множин $K_1, \ldots, K_v$, де K_i є сукупністю всіх секретних ключів абонента $i \in V$, отримаємо нерівність (14) (див. [42]).

Зазначені вище границі є загальними та дозволяють оцінити потенційну "потужність" методу "subset-cover framework", з точки зору можливості отримання на його основі ефективних схем багатоадресного розподілу ключів. Як показано в [7], за умовою "достатньо великих" значень параметру χ_t нижня границя (13) є "майже досяжною". Фактично це означає існування таких СБРК, що мають "достатньо велику" t-зв'язність, але надають можливість кожному учаснику зберігати "майже оптимальну" (згідно нерівності (13)) кількість секретних ключів, що він отримує з ЦРК. (Такі схеми багатоадресного розподілу ключів із структурою специфікації $(v - t, t)$, де $1 \leq t < v$, побудовані в явному вигляді; див. доведення теореми 20 з [7]).

Розробка більш раціональних методів синтезу безумовно стійких СБРК на основі систем множин, що дозволяють будувати схеми багатоадресного розподілу ключів із більш гнучким, потрібним на практиці співвідношенням між основними показниками їх ефективності, складає важливу задачу досліджень в галузі синтезу криптографічних протоколів розподілу ключів.

Один з можливих методів вирішення цієї задачі викладений в [6], де запропоновано будувати схеми багатоадресного розподілу ключів на основі неповних урівноважених блок-схем.

Нехай $D = (V, \widetilde{B})$ є довільною (b, v, r, k, λ)-конфігурацією (див. пункт 4). Тоді локальні ключові мережі відповідної СБРК D мають однакову потужність k, і кожний абонент $i \in V$ отримує з ЦРК рівно r секретних ключів; зокрема, справедлива рівність $n(D) = r$.

В [6] отримані аналітичні границі стійкості та t-зв'язності СБРК, що відповідає (b, v, r, k, λ)-конфігурації D:

$$r\lambda^{-1} < \tau(D),\ \chi_t(D) \le \frac{v-t}{r-\lambda t}(1+\ln k),\ 0 \le t < r\lambda^{-1}.$$

Також показано, що у випадку, коли D є проективною площиною порядку $k-1$, де $k \ge 3$ (тобто $k = r \ge 3$, $\lambda = 1$) [39], справедливі більш точні границі

$$\tau(D) = k-1,\ \chi_t(D) \le (k-1)(t+1),\ t \in \overline{0, \tau(D)}. \qquad (15)$$

Аналітичні співвідношення та границі стійкості СБРК D, що відповідає довільній (v, k, λ)-конфігурації (симетричній НУБС), отримані в [45]:

$$\left\lceil \frac{k}{\lambda} \right\rceil - 1 \le \tau(D) \le \frac{k}{\lambda}(1+\ln\lambda);$$

$$\tau(D) = \left\lceil \frac{k}{2} \right\rceil - 1, \text{ якщо } \lambda = 2;\ \tau(D) \le \left\lceil \frac{5k+1}{12} \right\rceil - 1, \text{ якщо } \lambda = 3.$$

В [50] на основі зазначених співвідношень та відомих необхідних умов існування симетричних блок-схем [39] запропонований алгоритм оцінки найменшого значення параметру $n(D)$ схеми багатоадресного розподілу ключів D, що має стійкість $\tau(D) \ge \tau_0$ та відповідає (v, k, λ)-конфігурації з параметром $v = v_0$, де v_0, τ_0 – довільні додатні цілочисельні константи.

Як показано в [6], використання НУБС в конструкціях СБРК, в ряді випадків, дозволяє суттєво зменшити кількість секретних ключів, що зберігає кожний абонент мережі зв'язку, за рахунок прийнятного збільшення довжини повідомлень, що передаються абонентам широкомовним каналом зв'язку з ЦРК, або навпаки. Так, у випадку, коли СБРК D основується на проективній площині порядку $k-1$, то її стійкість та кількість секретних ключів, що має кожний її учасник, дорівнюють відповідно $\tau(D) = O(\sqrt{v})$, $n(D) = O(\sqrt{v})$, $v \to \infty$. При цьому t-зв'язність даної СБРК складає $\chi_t(D) = O(t\sqrt{v})$, де $t < k = O(\sqrt{v})$, $v \to \infty$ (див. співвідношення (15)).

Поряд з тим, широке практичне застосування СБРК, що основуються на неповних урівноважених блок-схемах, вимагає подолання певних труднощів, які мають принциповий характер. Так, на сучасному етапі розвитку комбінаторної теорії не відомі загальні достатні умови існування НУБС із заданими значеннями параметрів [46]. З іншого боку, багато конкретних вивчених класів НУБС [39] не надають можливість отримувати схеми багатоадресного розподілу ключів із заданою (високою) стійкістю. Нарешті, співвідношення (1) між параметрами НУБС накладають занадто жорсткі обмеження на конструкції відповідних СБРК, що не дозволяє безпосередньо реалізовувати процедури приєднання нових учасників до таких схем розподілу ключів.

В роботах [51, 52] авторів цієї статті запропонований метод синтезу СБРК на основі покрить, які певним чином ставляться у відповідність блоковим

кодам над довільним скінченним алфавітом. На відміну від способу, що описаний в [6], новий метод синтезу СБРК є більш гнучким та надає більше можливостей для побудови безумовно стійких схем багатоадресного розподілу ключів із потрібними значеннями показників ефективності. Зокрема, як показано в [52], такий метод дозволяє будувати достатньо стійкі СБРК із загальним числом b секретних ключів, що не перевищує кількості v абонентів мережі зв'язку (відзначимо, що, згідно останнього співвідношення (1), це є принципово неможливим при побудові СБРК на основі НУБС).

Більш докладну інформацію про результати сучасних досліджень в галузі побудови схем багатоадресного розподілу ключів, що основуються на покриттях множини абонентів, можна знайти в [42 – 44].

Список литературы: **1.** *Конюшок С.М., Олексійчук А.М.* Безумовно стійкі схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: I. Схеми попереднього розподілу й узгодження ключів // Радіотехніка: Всеукр. міжвід. наук-техн. зб. **2.** *Fiat A., Naor M.* Broadcast encryption // Advances in Cryptology – EUROCRYPT'93, Lecture Notes in Computer Science. – 1994. – P. 480 – 491. **3.** *Stinson D.R.* On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243. **4.** *Cimato S., D'Arco P., Cresti A.* A unified model for unconditional secure key distribution // http://www.dia.unisa.it/paodar.dir. **5.** *Blundo C., D'Arco P., Daza V., Padro C.* Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures // ISC'01, Lecture Notes in Computer Science, Springer-Verlag. – 2001. – P. 1 – 17. **6.** *Korjik V., Ivkov M., Merinovich Y., Bang A., van Tilborg H.* A broadcast key distribution scheme based on block designs // Lecture Notes in Computer Science. – 1995. – № 1025. – P. 12 – 21. **7.** *Luby M., Staddon J.* Combinatorial bounds for broadcast encryption // Advances in Cryptology – EUROCRYPT'98, Lecture Notes in Computer Science. – 1998. – P. 512 – 527. **8.** *Berkovits S.* How to broadcast a secret // Advances in Cryptology – EUROCRYPT'91, Lecture Notes in Computer Science. – 1992. – P. 536 – 541. **9.** *Just M., Kranakis E., Krizanc D., van Oorschot P.* Key distribution via true broadcasting // 2nd ACM Conf. on Comp. and Communications Security. – 1994. – P. 81 – 88. **10.** *Blundo C., Cresti A.* Space requirements for broadcast encryption // Advances in Cryptology – EUROCRYPT'94, Lecture Notes in Computer Science. – 1994. – P. 287 – 298. **11.** *Blundo C., Frota Mattos L.A., Stinson D.R.* Multiple key distribution maintaining user anonymity via broadcast channels // J. of Comp. Security. – 1996. – Vol. 3. – P. 309 – 323. **12.** *Blundo C., Frota Mattos L.A., Stinson D.R.* Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution // Advances in Cryptology – CRYPTO'96, Lecture Notes in Computer Science. – 1996. – P. 387 – 400. **13.** *Padro C., Gracio I., Martin S., Morillo P.* Linear broadcast encryption schemes // Discrete Appl. Math. – 2003. – Vol. 128. – P. 223 – 238. **14.** *Stinson D.R., van Trung T.* Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. – 1998. – Vol. 15. – P. 261 – 279. **15.** *D'Arco P., Stinson R.D.* On unconditionally secure robust distributed key distribution centers // ASIACRYPT'02, Lecture Notes in Computer Science. – 2002. – P. 346 – 363. **16.** *Beimel A., Chor B.* Communication in key distribution schemes // IEEE Trans. on Inform. Theory. – 1996. – Vol. 42. – P. 19 – 28. **17.** *Alon N., Naor M.* Derandomization, witnesses for boolean matrix multiplication and constructions of perfect hash functions // Technical Report CS94-11. – Weizmann Institute of Science. **18.** *Gracia I., Martin S., Padro C.* Improving the trade-off betveen storage and communication in broadcast encryption schemes // http://www.iacr.org/2001/088. **19.** *Stinson D.R., Wei R.* An application of ramp schemes to broadcast encryption // Information Processing Letters. – 1999. – Vol. 69. – P. 131 – 135. **20.** *Stinson D.R.* An explication of secret sharing schemes // Designs, Codes and Cryptography. – 1992. – Vol. 2. – P. 357 – 390. **21.** *Seberry J., Charnes Ch., Pieprzyk J., Safavi-Naini R.* 41 Crypto topics and application // CRC Handbook of algorithms and theory of computation. – CRC Press.: Baca Raton, 1999. – P. 1 – 51. **22.** *Кабатянский Г.А.* Математика разделения секрета // Матем. Просвещение. – 1998. – Сер. 3, Вып. 2. – С. 115 – 126. **23.** *Shamir A.* How to share a secret //

Comm. ACM. – 1979. – Vol. 22, № 1. – P. 612 – 613. **24.** *Padro C., Gracia I., Martin S., Morillo P.* Linear key predistribution schemes // Designs, Codes and Cryptography. – 2002. – Vol. 25. – P. 281 – 298. **25.** *Eschenauer L., Glidor V.D.* A key management scheme for distributed sensor networks. // 9th ACM Conference on Comp. and Communication security. – 2002. – P. 41 – 47. **26.** *Lee J., Stinson D.R.* Deterministic key predistribution schemes for distributed sensor networks // SAC'04, Lecture Notes in Computer Science. – 2004. – P. 294 – 307. **27.** *Wei R., Wu J.* Product construction of key distribution schemes for sensor networks. // SAC'2004, Lecture Notes in Computer Science. – 2004. **28.** *Camtepe S.A., Yener B.* Combinatorial design of key distribution mechanisms for wireless sensor networks. // Lecture Notes in Computer Science. – 2004. – Vol. 3193. – P. 293 – 308. **29.** *Lee J., Stinson D.R.* A combinatorial approach to key predistribution for distributed sensor networks // WCNC'05. – 2005. **30.** *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с. **31.** *Mitchell C.J., Piper F.C.* Key storage in secure networks // Discrete Applied Mathematics. – 1998. – Vol. 21. – P. 215 – 228. **32.** *Dyer M., Fenner T., Frieze A., Thomason A.* On key storage in secure networks. // J. of Cryptology. – 1995. – Vol. 8. – P. 189 – 200. **33.** *Matsumoto T.* Incidence structures for key sharing // ASIACRYPT'94, Lecture Notes in Computer Science. – 1995. – P. 342 – 353. **34.** *Фомичев В.М.* Дискретная математика и криптология. Курс лекций. – М.: Диалог-МИФИ, 2003. – 400 с. **35.** *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с. **36.** *Carter J.L., Wegman M.N.* Universal classes of hash functions // J. of Comp. and System Sciences. – 1979. – Vol. 18. – P. 143 – 154. **37.** *Левин Л.А.* Односторонние функции // Проблемы передачи информации. – 2003. – Т. 39, Вып. 1. – С. 103 – 117. **38.** *Вербіцький О.В.* Вступ до криптології. – Львів: ВНТЛ, 1998. – 247с. **39.** *Холл М.* Комбинаторика: Пер. с англ. – М.: Мир, 1970. – 427 с. **40.** *Stinson D.R.* Combinatorial designs: constructions and analysis. – New-York, Springer-Verlag, 2003. **41.** *Blundo C., de Santis A., Herzberg A., Kutten S., Vaccaro U., Yung M.* Perfectly-secure key distribution for dynamic conferences // Advances in cryptology – CRYPTO'92, Lecture Notes in Computer Science. – 1993. – P. 471 – 486. **42.** *Naor D., Naor M., Lotspiech J.* Revocation and tracing schemes for stateless receivers // Advances in Cryptology – CRYPTO'01, Lecture Notes in Computer Science. – 2001. – P. 41 – 62. **43.** *Attrapadung N., Kobara K., Imai H.* Sequential key derivation patterns for broadcast encryption and key predistribution schemes // ASIACRYPT'03, Lecture Notes in Computer Science. – 2003. – P. 374 – 391. **44.** *Halevy D., Shamir A.* The LSD broadcast encryption scheme // Advances in Cryptology – CRYPTO'02, Lecture Notes in Computer Science. – 2002. – P. 47 – 60. **45.** *Алексейчук А.Н., Паничек В.Г.* Анализ стойкости ключевых сетей относительно компрометации корреспондентов // Збірник наукових праць КВІУЗ. – Вип. 3. – Київ, 1998. – С. 76 – 83. **46.** *Сачков В.Н., Тараканов В.Е.* Комбинаторика неотрицательных матриц. – М.: ТВП, 2000. – 447с. **47.** *Naor M., Pincas B.* Efficient trace and revoke schemes // FC'00, Lecture Notes in Computer Science. – 2000. – P. 1 – 20. **48.** *Wallner D.M., Harder E.J., Agee R.C.* Key management for multicast: issues and architectures // ftp://ftp.ieft.org/internet-drafts/draft-wallner-key-arch-01.txt. **49.** *Erdos P., Rado R.* Intersection theorem for systems of sets // J. London Math. Soc. – 1960. – Vol. 35. – P. 85 – 90. **50.** *Конюшок С.М.* Алгоритм оцінки параметрів оптимальних ключових структур, побудованих на основі неповних урівноважених блок-схем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 6. – Київ, 2003. – С. 79 – 83. **51.** *Алексейчук А.Н., Конюшок С.Н.* Асимптотические соотношения для вероятностей числа нескомпрометированных ключей в схемах распределения ключей, построенных на основе блоковых кодов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Вип. 8. – Київ, 2004. – С. 85 – 90. **52.** *Алексейчук А.Н., Конюшок С.Н.* Безусловно стойкая схема многоадресного распределения ключей, построенная на основе блоковых кодов // Збірник матеріалів Четвертої міжнар. конф. „ІНТЕРНЕТ – ОСВІТА – НАУКА – 2004". – Вінниця: УНІВЕРСУМ-Вінниця, 2004. – Т. 2. – С. 492 – 494.