УДК 621.391:519.854

АЛГОРИТМ ОЦІНКИ ПАРАМЕТРІВ ОПТИМАЛЬНИХ КЛЮЧОВИХ СТРУКТУР, ЩО ПОБУДОВАНІ НА ОСНОВІ НЕПОВНИХ УРІВНОВАЖЕНИХ БЛОК-СХЕМ

Сергій Конюшок

СФ СБ України у складі ВІТІ НТУУ "КПІ"

Анотація: **Проведені дослідження ефективності (за показниками стійкості та кількості ключів, що має кожний кореспондент) структур мереж засекреченого зв'язку, які побудовані на основі неповних урівноважених блок-схем. Розроблений алгоритм оцінки значень параметрів оптимальних ключових структур, які задовольняють вимогам щодо стійкості та мінімальності числа ключів, що має кожний кореспондент мережі зв'язку.**

Summary: **The research of the effectiveness (for he security index and the quantity of keys for each correspondent) of the network structures for confidential telecommunications on the base of balanced incomplete block designs was made. The algorithm for the evaluation of the parameter values of the optimal key requirements for security and minimality of the keys for each network correspondent.**

Ключові слова: **ключова мережа, компрометація, криптоживучість, стійкість ключової мережі до компрометацій кореспондентів, неповна урівноважена блок-схема.**

I. Вступ

З розширенням використання комп'ютерних мереж, зокрема, глобальної мережі Інтернет та появою нових потужних комп'ютерів, технологій мережевих і нейронних обчислень однією з найбільш актуальних задач в галузі криптографічного захисту інформації є розробка нових способів побудови ключових структур мереж засекреченого зв'язку (ключових мереж (КМ)) з заданими параметрами по їх криптоживучості, які дозволяють автоматизувати процеси планування та побудови цих структур [1, 2]. Зазначений факт можна пояснити стрімким зростанням масштабів і складності розв'язуваних задач, збільшенням кількості напрямків зв'язку в сучасних телекомунікаційних системах, а також необхідністю обліку при плануванні великої кількості зовнішніх і внутрішніх факторів, що впливають на умови функціонування мереж зв'язку.

На сьогодняшний день відомі різноманітні математичні моделі та методи побудови ключових структур мереж засекреченого зв'язку [1 – 3], з використанням яких розроблені протоколи розподілу ключів в зазначених мережах, що враховують, зокрема, особливості їх функціонування в умовах компрометацій кореспондентів. Наприклад, в [2] отримані оцінки витрат ключової інформації при компрометації кореспондентів мережі. Також введені критерії стійкості базисної інформації кореспондентів мережі до компрометації одного з кореспондентів.

Взагалі, проблемам планування та побудови, моніторингу та керування ключовими мережами присв'ячено велика кількість публікацій (див., наприклад, [1 – 5]). Запропоновано багато ефективних рішень задач, що виникають, але, незважаючи на безупинне збільшення обсягу наукових робіт з організації і забезпечення планування та побудови КМ, цей процес, серед йому подібних, є найменш автоматизованим.

II. Постановка задачі

Один із загальних підходів до підвищення криптоживучості КМ, що дозволяють, у ряді випадків, забезпечити прийнятне поєднання стійкості, гнучкості та практичності керування ключами, полягає у декомпозиції множини кореспондентів (ключів) мережі зв'язку на низку ієрархічно впорядкованих локальних підгруп з наступною реалізацією відносно автономного керування ключами у кожній підгрупі [4, 5]. Природним є використання в якості математичної моделі ключової структури мережі зв'язку, що складається з локальних підгруп (ключових мереж), комбінаторної конфігурації [6] на множині кореспондентів мережі. Широкий клас таких конфігурацій, що описують ключові мережі, ведено в розгляд в статті [7]. Там же визначено поняття стійкості КМ відносно компрометацій кореспондентів та отримані оцінки стійкості ключових мереж, зокрема, КМ, що побудовані на основі симетричних неповних урівноважених блок-схем (НУБС) [8].

Відмітимо, що на даний час симетричні блок-схеми складають один з найбільш вивчених класів комбінаторних конфігурацій, для побудови і дослідження властивостей яких розроблені різноманітні

ефективні та глибокі методи [6, 8]. Тому, вибір НУБС в якості моделей ключових структур мереж засекреченого зв'язку вважається цілком виправданим, як з теоретичної, так і практичної точки зору.

До найважливіших задач аналізу та синтезу КМ, що моделюються за допомогою комбінаторних конфігурацій, відноситься розробка ефективних алгоритмів оцінки параметрів та методів побудови блок-схем, що реалізують ключові структури, які мають максимальну стійкість відносно компрометацій або мінімальну кількість ключів, що зберігаються у кожного кореспондента мережі, при заданих нижніх межах стійкості (такі структури названо нижче t-оптимальними).

В даній статті розроблений алгоритм оцінки параметрів оптимальних ключових структур, що побудовані на базі симетричних НУБС, який допускає ефективну програму реалізацію та може бути безпосередньо використаний під час планування та попереднього аналізу властивостей ключових структур мереж засекреченого зв'язку.

III. Основна частина

Наведемо формальні визначення основних понять та деякі результати, що отримані в [7], які використовуються далі в статті. Математична модель ключової мережі, що запропонована в [7], являє собою конфігурацію (сукупність підмножин) $D = \{B_1, B_2, \ldots, B_b\}$ кінцевої множини $\{1, 2, \ldots, v\}$, яка задовільняє наступним умовам:

1. Кожна підмножина B_l, $l \in \overline{1,b}$ містить не менш двох елементів.
2. Кожна пара елементів $i, j \in \overline{1,v}$ належить щонайменше до однієї підмножини.
3. Будь-які дві підмножини мають непорожній перетин.

Елементи $1, 2, \ldots, v$ називаються кореспондентами ключової мережі. Множини $B_1, \ldots, B_b$ звуться локальними ключовими мережами (ЛКМ). Кореспонденти, що належать одній ЛКМ, мають одинакові ключі, які використовуються ними для зв'язку в рамках даної ЛКМ. Таким чином, з кожною ЛКМ пов'язаний певний ключ, причому різним ЛКМ відповідають різні ключі.

Відзначимо, що умова 3 гарантує можливість зв'язку між будь-якою парою (i, j) кореспондентів на будь-яких наявних у їхньому розпорядженні ключах, оскільки завжди існує кореспондент k, що володіє як наперед заданим ключем кореспондента i, так і наперед заданим ключем кореспондента j.

За визначенням, компрометація i-го $(i \in \overline{1,v})$ кореспондента означає, що з конфігурації D виключаються всі ЛКМ, що містять i, тобто ключі, що належать i-му кореспонденту не можуть бути використані для зв'язку між іншими кореспондентами КМ [2]. Стійкістю [7] $\tau(D)$ ключової мережі D називається найбільше натуральне число t таке, що при компрометації будь-яких t кореспондентів даної КМ між будь-якими двома з решти $v - t$ кореспондентів може бути забезпечений зв'язок. Таким чином, стійкість КМ визначає надійність зв'язку між кореспондентами в умовах, коли деякі з них скомпрометовані.

Як зазначено вище, з теоретичної та практичної точок зору, існує необхідність дослідження стійкості КМ, що реалізовані на базі симетричних неповних урівноважених блок-схем ((v, k, λ)-конфігурацій) [8]. В таких ключових мережах кореспондентами є елементи блок-схеми, а кожну ЛКМ представляє відповідний блок даної схеми. При цьому параметри v, k, λ симетричної блок-схеми, якій відповідає ключова мережа, позначають наступне [7]:

v – загальна кількість кореспондентів КМ та кількість локальних ключових мереж;

k – кількість ЛКМ, яким належить кожен кореспондент мережі (кількість ключів, що має кореспондент, а також [8] потужність довільної ЛКМ);

λ – кількість ЛКМ, яким належить кожна пара різних кореспондентів мережі.

З практичних та економічних міркувань, зрозумілою є необхідність забезпечення максимальної стійкості ключової мережі до компрометацій при мінімальній кількості ключів, що має кожний кореспондент. З метою точного визначення таких структур введемо основні кількісні показники.

Для будь-якого натурального v позначимо $\theta(v)$ як максимальне натуральне число t, для якого існує (v, k, λ)-конфігурація D, що задовільняє умові $\tau(D) \geq t$. Аналогічно, для будь-яких v і t з множини натуральних чисел позначимо через $k(v, t)$ мінімальне натуральне число k, для якого існує (v, k, λ)-конфігурація D така, що $\tau(D) \geq t$.

Визначення. Назвемо t-*оптимальною структурою* ключову мережу $\tilde{D}$, що побудована на основі блок-схеми з параметрами ($v, \tilde{k}, \tilde{\lambda}$) та задовільняє умовам $\tau(\tilde{D}) \geq t$, $\tilde{k} = k(v, t)$. Якщо $t = \theta(v)$, то t-оптимальну структуру будемо називати *оптимальною*.

Отже, з сімейства (v, k, λ)-конфігурацій D із заданим v, стійкість $\tau(D)$ яких не менша деякого числа t, будемо називати t-оптимальною таку структуру, що має найменше значення k серед всіх конфігурацій даного сімейства. За визначенням, оптимальними є такі структури, що володіють максимальною стійкістю $\theta(v)$ при мінімальній кількості ключів, що має кожний кореспондент мережі.

Розроблений у статті алгоритм оцінки значень параметрів $\theta(v)$ та $k(v, t)$ базується на наступних результатах.

Теорема 1. Нехай ключова мережа D є (v, k, λ)-конфігурацією. Тоді

$$\left\lceil \frac{k}{\lambda} \right\rceil - 1 \leq \tau(D) \leq \frac{k}{\lambda}(1 + \ln \lambda), \tag{1}$$

$$\tau(D) = k - 1, \text{ якщо } \lambda = 1; \tag{2}$$

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

$$\left\lceil \frac{k}{3} \right\rceil - 1 \leq \tau(D) \leq \left\lceil \frac{5k+1}{12} \right\rceil - 1, \text{ якщо } \lambda = 3. \tag{4}$$

Верхня межа в формулі (1) витікає з оцінки потужності мінімального покриття кінцевої множини її підмножинами [9]. Решта результатів отримані в статті [7].

Теорема 2. Нехай існує (v, k, λ)-конфігурація D така, що $\tau(D) \geq t$. Тоді справедливі нерівності

$$\frac{v+t}{t+1} \leq k(v,t) \leq v - 2. \tag{5}$$

Верхня межа (5) витікає з властивостей симетричних блок-схем. Для доведення нижньої границі розглянемо систему співвідношень (див. (1))

$$\begin{cases} \dfrac{k}{\lambda} - 1 \leq t, \\ k(k-1) = \lambda(v-1). \end{cases} \tag{7}$$

В результаті нескладних перетворень

$$\begin{cases} \dfrac{k}{\lambda} - 1 \leq t, \\ k(k-1) = \lambda(v-1), \end{cases} \Leftrightarrow \begin{cases} \dfrac{k}{\lambda} \leq t+1, \\ \dfrac{k}{\lambda} = \dfrac{v-1}{k-1}, \end{cases} \Leftrightarrow \begin{cases} \dfrac{k}{\lambda} = \dfrac{v-1}{k-1}, \\ \dfrac{v-1}{k-1} \leq t+1, \end{cases} \Leftrightarrow \begin{cases} \dfrac{k}{\lambda} = \dfrac{v-1}{k-1}, \\ v-1 \leq (t+1)(k-1), \end{cases} \Leftrightarrow \begin{cases} \dfrac{k}{\lambda} = \dfrac{v-1}{k-1}, \\ \dfrac{v+t}{t+1} \leq k \end{cases}$$

отримаємо нижню границю (5) параметру $k(v, t)$.

Сформулюємо необхідну умову існування симетричної НУБС з заданими параметрами, що використовується в алгоритмі.

Теорема Брука-Райзера-Човла [8]. Якщо існує симетрична урівноважена неповна блок-схема з параметрами v, k, λ, то

а) при v парному $k - \lambda$ є квадратом;

б) при v непарному рівняння

$$x^2 = (k-\lambda)y^2 + (-1)^{(v-1)/2} \lambda z^2 \tag{8}$$

має рішення в цілих числах, що одночасно не рівні нулю.

Для перевірки умови б) застосовується теорема Лежандра [10], яка дає відповідь на питання, чи має рівняння виду

$$ax^2 + by^2 + cz^2 = 0 \tag{9}$$

нетривіальне цілочислове рішення.

Нехай $(k-\lambda)'$ та λ' позначають відповідно вільні від квадратів частини чисел $k-\lambda$ та λ, d позначає найбільший спільний дільник чисел $(k-\lambda)'$ та λ'. Рівняння (8) має рішення в цілих x, y, z, не рівних нулю одночасно, тоді і тільки тоді, коли рівняння

$$dx^2 = \frac{(k-\lambda)'}{d} y^2 + (-1)^{\frac{v-1}{2}} \frac{\lambda'}{d} z^2 \tag{10}$$

має ненульове ціле рішення (x, y, z). При цьому рівняння (10) є рівнянням Лежандра виду (9). Таким чином, якщо при непарному v існує (v, k, λ)-конфігурація, то по теоремі Лежандра числа

$$(-1)^{\frac{v+1}{2}} \frac{\lambda'(k-\lambda)'}{d^2}, \quad (-1)^{\frac{v-1}{2}} \lambda', \quad (k-\lambda)' \tag{11}$$

є квадратичними лишками по модулям d, $\frac{(k-\lambda)'}{d}$, $\frac{\lambda'}{d}$ відповідно. Слід також особливо підкреслити, що при непарному v та найбільшому спільному дільнику чисел k та λ, рівному 1, число $(-1)^{\frac{v-1}{2}} \lambda'$ є квадратичним лишком по модулю $(k-\lambda)'$.

Спираючись на перераховані вище результати, опишемо *алгоритм оцінки параметрів* $\theta(v)$ *та* $k(v, t)$ *оптимальних ключових структур, що побудовані на основі НУБС, при заданій кількості* v *кореспондентів мережі зв'язку.*

Алгоритм представляє собою три етапи, що виконуються послідовно. На першому етапі для даного v визначаються параметри k та λ блок-схеми. Для цього організовано два вложених цикли. Спочатку відбувається перебор значень t $(1 \le t \le v-3)$ від максимального значення до мінімального. Для кожного значення t обраховуються (відповідно теоремі 2) границі параметру k, в межах яких перебор ведеться від меншої величини до більшої. При відомих v та k з використанням властивостей симетричних НУБС знаходимо λ

$$\lambda = \frac{k(k-1)}{v-1}. \tag{12}$$

Якщо λ ціле, то відбувається перехід до наступних етапів алгоритму, які виконуються в тілі даних циклів (по t та k відповідно), в протилежному випадку – значення k збільшується на 1.

На другому етапі відбувається перевірка умов існування блок-схеми з заданими параметрами k та λ, значення яких отримані на першого етапі алгоритму. З цією метою використовується теорема Брука-Райзера-Човла. В алгоритмі застосовується перевірка існування цілочисельних рішень рівняння (10) з використанням (11). За невиконання умов теореми відбувається перехід до чергового значення параметру k. В разі, якщо умови виконуються, відбувається перехід до наступного етапу.

На третьому етапі алгоритму для отриманих значень t, k та λ, які обчислені раніше, здійснюється перевірка співвідношень (1) – (4) (оцінка стійкості КМ, яка побудована на основі (v, k, λ)-конфігурації). Для такої перевірки параметр t розглядається як значення стійкості до компрометації кореспондентів $\tau(D)$ відповідної ключової структури D. У випадку, якщо значення параметрів не задовільняють даним співвідношенням, то робота алгоритму починається для наступного значення k. Блок-схема, яка задовольняє всім перерахованим вимогам (якщо вона існує), представляє собою модель ключової структури з заданою кількістю кореспондентів v та розрахованими верхньою границею стійкості $\theta(v)$ та нижньою границею параметра $k(v, t)$.

Таким чином, результатом роботи алгоритму є отримані оцінки параметрів $\theta(v)$ та $k(v, t)$ неповних урівноважених блок-схем, що задовольняють вимогам по стійкості до компрометацій кореспондентів. В табл. 1 приведені результати розрахунків меж параметрів $\theta(v)$, $k(v, t)$ для ряду значень v.

Таблиця 1

Оцінки параметрів оптимальних ключових структур
для деяких значень v кількості абонентів мережі

v	$t \geq \theta(v)$	$k \leq k(v, t)$	λ
7	2	3	1
11	2	5	2
13	3	4	1
15	4	8	4
15	2	7	3
16	2	6	2
19	5	10	5
19	4	9	4
21	4	5	1
22	3	7	2
23	5	11	5
25	3	9	3
27	5	13	6
29	3	8	2
31	6	16	8
31	5	6	1
34	7	12	4
35	6	17	8

Розглянемо отримані результати. В першу чергу, слід наголосити, що розраховані значення k та t (див. табл. 1) є нижньою та верхньою оцінкою параметрів $k(v,\ t)$ та $\theta(v)$ відповідно. Зокрема, стійкість $\theta(v)$ оптимальної структури не може перевищувати значення t, яке отримане з використанням запропонованого алгоритму. З іншого боку, значення стійкості накладає свої обмеження на кількість ключів, що мають кореспонденти мережі зв'язку. При кількості ключів k_0, меншим значення k, що знайдено за допомогою алгоритму, стійкість ключової мережі з параметрами $(v,\ k_0,\ \lambda)$ (якщо вона існує) є менш ніж t. Окремим випадком є НУБС з параметром $\lambda = 1$ або $\lambda = 2$, для яких відомі точні значення стійкості, тому для зазначених λ отримані оцінки чисел $k(v,\ t)$ та $\theta(v)$ є точними. Таким чином, якщо для заданого v з використанням алгоритму отримані параметри $(v,\ k,\ 1)$- або $(v,\ k,\ 2)$-конфігурацій, то (при умові існування) конфігурації з такими параметрами реалізують оптимальні структури мереж зв'язку, які володіють максимальною стійкістю при мінімальній кількості ключів, що має кожен кореспондент мережі.

З числа значень v, які вказані в таблиці, цікавим випадком є значення $v = 15$, що демонструє іншу важливу властивість алгоритму – він є досить гнучким до зміни вимог по стійкості. Так, зменшення t дозволяє визначити параметри блок-схеми із меншим значенням $k(v,\ t)$, тобто з меншою кількістю ключів кореспондента, що спрощує створення КМ на основі зазначеної блок-схеми (у випадку її існування).

IV. Висновки

Запропонований алгоритм дозволяє оцінити значення параметрів $\theta(v)$, $k(v,\ t)$ відповідно оптимальних та t-оптимальних ключових структур мереж зв'язку та довести неможливість побудови на основі довільних $(v,\ k,\ \lambda)$-конфігурацій ряду ключових мереж із заданими кількістю v кореспондентів та стійкістю t. Алгоритм може бути використаний на етапах проектування та попереднього аналізу властивостей мереж зв'язку, ключові структури яких є неповними урівноваженими блок-схемами. На думку автора, застосування цього алгоритму дозволить спростити процес планування ключових мереж, що задовільняють вимогам щодо стійкості, загальній кількості кореспондентів та мінімальності числа ключів, що має кожний кореспондент мережі.

Література: 1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.:Триумф, 2002. – 816 с. 2. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН – Р, 2002. –

512 с. 3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии М.: Гелиос АРВ. 2001.- 480с.4. Wong C.K, Gauda M., Lam S.S. Secure Group Communications Using Key Graphs // Proceedings of the ACM SIGCOMM '98, Vancouver, B.C., September 1998. 5.Mittra S. Iolus: A Framework for Scalable Secure Multicasting // Proceedings of the ACM SIGCOMM '97, September 14 – 18, 1997. 6.. Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц. – М.: ТВП, 2000. – 447с. 7. Алексейчук А.Н., Паничек В.Г. Анализ стойкости ключевых сетей относительно компрометации корреспондентов // Збірник наукових праць КВІУЗ. – Вип. 3. – Київ, 1998. – С. 76 – 83. 8. Холл М. Комбинаторика. Пер. с англ. – М.: Мир, 1970. – 427 с. 9. Нигматуллин Р.Г. Метод наискорейшего спуска в задачах на покрытие // Вопросы точности и эффективности вычислительных алгоритмов – Вып. 5: труды симпозиума. – Киев,1969. – С. 116 – 126. 10. Райзер Г. Дж. Комбинаторная математика. Пер. с англ. – М.: Мир, 1966. – 156 с.