DOI 10.20535/2411-1031.2025.13.2.344838
УДК 004.056

ВАЛЕРІЙ ЗАКУСІЛО,
СЕРГІЙ КОНЮШОК

АЛГОРИТМ ВІДСТЕЖУВАННЯ ПОРУШНИКІВ В СХЕМАХ БАГАТОАДРЕСНОГО РОЗПОДІЛУ КЛЮЧІВ

Стаття присвячена дослідженню рандомізованих схем багатоадресного розподілу ключів, побудованих на основі кодових конструкцій, та їх застосуванню для реалізації схем відстежування порушників (traitor tracing). Схема багатоадресного розподілу ключів – це криптографічний протокол, в якому центр розподілу ключів здійснює передачу певної допоміжної інформації (доступ до якої повинні мати тільки авторизовані користувачі) абонентам мережі зв'язку так, що з часом, в разі компрометації криптографічних ключів частини абонентів, перелік яких центру розподілу ключів вдалося встановити, інші абоненти зможуть відновити спільний криптографічний ключ, який в зашифрованому вигляді передається з центру розподілу ключів по широкомовному каналу зв'язку. При цьому, абоненти, ключі яких були скомпрометовані, не зможуть розшифрувати передане широкомовне повідомлення. Як видно, для успішного функціонування таких схем, існує потреба в підходах та інструментах встановлення переліку скомпрометованих абонентів (для різних задач може бути потреба як в повному переліку таких абонентів, так і хоча б одного з них). Класичні схеми traitor tracing можуть стати основою для побудови таких інструментів оскільки створювались для виявлення користувача або групи недобросовісних користувачів, які передали свої ключі для створення масиву скомпрометованих ключів, яким можуть скористатись в зловмисних цілях (так званого "декодера порушника"). Однак, в умовах зростання кількості абонентів, стрімкого розвитку обчислювальних ресурсів, створення адаптивних атак та зростання вимог до приватності, такі схеми демонструють зниження ефективності.

Запропонований у статті підхід спрямований на поєднання можливостей схем багатоадресного розподілу ключів і схем відстежування порушників з дотриманням балансу між точністю відстежування порушників та ефективністю доступних обчислювальних ресурсів. Завдяки застосуванню оцінок Геффдінга побудований в статті алгоритм є t-ідентифікуючим, тобто здатен гарантувати ідентифікацію хоча б одного учасника будь-якої коаліції, що не перевищує t порушників. Наведені достатні умови на параметри кодів забезпечують суттєве покращення порівняно з класичними. Продемонстровано, що рандомізований підхід зберігає рівень стійкості системи і не погіршує безпекових властивостей оригінальної схеми, але істотно підсилює її здатність розрізняти користувачів у випадку компрометації ключів. Отримані в статті аналітичні вирази дозволяють отримати точні нижні оцінки надійності алгоритму відстежування порушників, що, в свою чергу, може бути використане при практичній побудові рандомізованих протоколів відстежування з заданою необхідною (високою) надійністю.

Ключові слова: кібербезпека; кіберзахист; криптографія; traitor tracing; схема багатоадресного розподілу ключів.

Постановка проблеми. З розвитком цифрових технологій та поширенням розподілених систем зберігання даних, суттєво зростає ризик несанкціонованого доступу та витоку інформації. Незважаючи на значний прогрес у методах шифрування та автентифікації,

проблема встановлення відповідальності за порушення (зокрема, в разі змови декількох користувачів) залишається відкритою. Схеми відстежування порушників (*traitor tracing schemes*) покликані заповнити цю прогалину, дозволяючи з високою ймовірністю ідентифікувати джерело витоку. Однак класичні підходи часто не враховують особливості сучасних сценаріїв використання – наявність великої кількості користувачів, розподіленість даних, динамічність ключової інфраструктури. Крім того, практичне впровадження таких систем стикається з низкою проблем – високими обчислювальними витратами та складністю доведення безпеки.реалізуються при неповній або розмитій інформації про систему та її механізми захисту, що ускладнює їх своєчасне виявлення та оцінку.

Аналіз останніх досліджень і публікацій. Проблематика захисту широкомовного контенту виникла задовго до формалізації traitor tracing. У 1970-1980-х роках основна увага приділялася схемам broadcast encryption, які давали змогу ефективно виключати окремих абонентів із доступу до зашифрованого потоку. Класичним прикладом є робота Fiat і Naor 1987 року, де запропоновано моделі revocation schemes на основі односпрямованих функцій [1].

Мотивація походила переважно з індустрії платного телебачення. Оператори кабельних мереж стикалися з клонуванням смарт-карт і декодерів, що призводило до значних фінансових втрат. Проте на той час трасування розглядалося лише як побічний ефект механізмів відкликання ключів, а не як самостійна криптографічна задача. Відсутність формальної моделі коаліційних атак обмежувала розвиток систематичного підходу.

Формальна модель traitor tracing була вперше представлена в статті Benny Chor, Amos Fiat і Moni Naor на конференції CRYPTO 1994 під назвою “Tracing Traitors” [2]. Автори ввели чітке визначення системи з n користувачами, де коаліція розміром не більше t порушників може створити піратський декодер. Алгоритм відстежування мав ідентифікувати принаймні одного учасника коаліції з високою ймовірністю.

Запропонована схема базувалася на інтерполяції многочленів, подібно до секретного розподілу Shamir. Кожен користувач отримував точку на кривій, а піратський декодер розкривав достатньо інформації для відновлення принаймні однієї з точок. Робота розрізняла ймовірнісне та детерміноване відстежування, заклавши основи для подальших досліджень. Значення статті полягає в переході від пасивного відкликання до активного виявлення порушників.

Подальший розвиток зосередився на підвищенні ефективності та розширенні криптографічних припущень. У 1997 році Boneh і Franklin представили першу схему traitor tracing з публічним ключем, що усунула потребу в захищеному каналі для дистрибуції ключів [3]. Їх підхід інтегрував ідеї identity-based encryption і дав змогу масштабувати систему до великих аудиторій.

Kurosawa і Desmedt у 1998 році оптимізували розмір ключів, запропонувавши компактніші структури на основі комбінаторних методів [4]. Паралельно розвивалися моделі black-box і non-black-box відстежування: перша передбачала доступ лише до поведінки декодера, друга – до його внутрішньої структури. Незважаючи на теоретичні успіхи, практичне впровадження гальмувалося через великі обсяги ключової інформації та повільне відстежування.

На початку 2000-х traitor tracing почав інтенсивно перетинатися з теорією кодування. Проривною стала робота Gabor Tardos 2003 року, де введено ймовірнісні коди з оптимальною довжиною для задачі fingerprinting [5]. Коди Tardos ґрунтуються на мінімізації ймовірності помилкового звинувачення та забезпечують стійкість проти коаліцій розміром до квадратного кореня від кількості користувачів.

Ці ідеї були адаптовані до відстежування шляхом вбудовування кодових слів у ключі абонентів. Гібридні моделі, натхненні collusion-resistant кодами Boneh-Shaw [6], дали змогу поєднувати криптографічні та кодувальні підходи. Практичним результатом стало

впровадження принципів traitor tracing у систему AACS для захисту Blu-ray дисків, запущену в 2005 році.

Останнє десятиліття характеризується переходом до постквантових конструкцій та інтеграцією з розширеними примітивами. З 2015 року активно досліджуються схеми на основі ґрат, стійкі до атак Шора [7]. Паралельно traitor tracing вбудовується в attribute-based encryption, що дає змогу гнучко керувати політиками доступу [8].

Значним кроком стало досягнення повного black-box confirmation, продемонстроване Garg та іншими у 2020 році [9]. Така схема гарантує ідентифікацію порушника навіть без фізичного доступу до декодера. У комерційному секторі принципи частково реалізовано в Microsoft PlayReady та Google Widevine. Останнім трендом є децентралізовані схеми на основі блокчейну [10], що досліджуються з 2020 року для застосувань у Web3.

Метою статті є розробка та дослідження підходу, орієнтованого на досягнення балансу між точністю відстежування порушників та ефективністю доступних обчислювальних ресурсів за рахунок синтезу рандомізованого алгоритму відстежування порушників по схемам багатоадресного розподілу ключів, що основуються на кодових конструкціях.

Виклад основного матеріалу дослідження. Нагадаємо, що схема багатоадресного розподілу ключів (СБРК) [11] являє собою криптографічний протокол, за допомогою якого довірена сторона, що виконує функції центру розподілу ключів, здійснює передачу певної допоміжної секретної інформації абонентам мережі зв'язку так, що з часом абоненти, які входять до певної привілейованої коаліції, можуть відновити спільний секретний ключ, який в зашифрованому вигляді передається з центру розподілу ключів по широкомовному каналу зв'язку.

Далі у статті вільно використовуються поняття, що визначені в [11]. Нехай V – множина абонентів мережі зв'язку, $|V| = \upsilon$, $B = \{B_1, B_2, ..., B_b\}$ – покриття множини V, D – СБРК, що відповідає конфігурації (V, B). Ототожнимо блоки покриття B з їх номерами, тобто числами $1, 2, ..., b$. Нагадаємо, що кожне з цих чисел є ідентифікатором деякого секретного ключа в схемі D.

Позначимо $K_x = \left\{ j \in \overline{1,b} : x \in B_j \right\}$ множину ідентифікаторів ключів, що зберігається у абонента $x \in V$. Припустимо, що $|K_x| = n$ для будь-якого $x \in V$.

Нехай

$$C \subseteq V, |C| = t, H \subseteq \bigcup_{x \in C} K_x, |H| = N \geq n. \quad (1)$$

Нижче множина абонентів C інтерпретується як коаліція порушників, а множина ідентифікаторів ключів H – як піратський декодер.

Алгоритм відстежування порушників в СБРК D полягає в пошуку хоча б однієї частини коаліції C за вхідною множиною H. Цей алгоритм складається з наступних кроків:

1) обчислити значення:

$$\upsilon_x = |H \cap K_x|, x \in V; \quad (2)$$

2) сортувати їх по незростанню;

3) оголосити порушником таку частину $x^* = x^*(C, H)$, для якої значення V_{x^*} максимальне.

Зрозуміло, що даний алгоритм помиляється тоді і тільки тоді, коли знайдений елемент x^* не належить множині C.

Назвемо СБРК D t-ідентифікуючою, якщо для будь-якої пари множин (C, H), що задовільняє умову (1), виконується відношення $x^*(C, H) \in C$.

В роботі [12] запропоновано спосіб побудови схем відстежування порушників, посилаючись на схеми розподілу ключів. Застосовуючи до СБРК D, цей спосіб полягає в

наступному: нехай B' – множина потужності mb, $\sigma: B' \to B$ – відображення таке, що $\left|\sigma^{-1}(j)\right| = m$ для будь-якого $j \in B$.

Елементи множини B' є ідентифікаторами секретних ключів нової СБРК D', яка відповідає СБРК D та відображення σ.

На першому етапі СБРК D' кожний абонент $x \in V$ отримує набір з n секретних ключів, які формуються наступним чином. Нехай $j_1(x),\ldots,j_n(x) \in \overline{1,b}$ – ідентифікатори ключів абонента x у вихідній СБРК D, записані в певному фіксованому порядку. Пронумеруємо елементи множини V числами від 1 до υ і розглянемо послідовність незалежних випадкових величин $\eta_{j_l(x)}$, $x \in \overline{1,\upsilon}$, $l \in \overline{1,n}$, рівномірно розподілених на множині $\overline{1,m}$. Тоді ідентифікаторами секретних ключів абонента x в СБРК D' є випадкові елементи множини B', l-ий з яких дорівнює $\eta_{j_l(x)}$-му по рахунку елементу множини $\sigma^{-1}(j_l(x))$, $l \in \overline{1,n}$. Таким чином, загальна кількість секретних множин СБРК D' дорівнює mb, і ці ключі (при передачі їх абоненту, вибираються випадковим чином, рівноймовірно та незалежно один від одного, при чому кожен ключ з ідентифікатором $j \in B$ ділиться на m секретних ключів в новій СБРК, ідентифікатори яких утворюють множину $\sigma^{-1}(j)$.

Нехай тепер, на 2-му етапі, потрібно передати багатоадресне повідомлення m_P коаліції $P \subseteq V$. Нехай $i_1,\ldots,i_s$ – ідентифікатор секретних ключів в СБРК D, використовується для зашифрування m_P в цій схемі розподілу ключів. Тоді в СБРК D' повідомлення m_P зашифровується на всіх ключах, ідентифікатори яких належать об'єднанню $\bigcup_{j=1}^{s} \sigma^{-1}(i_j)$.

Таким чином, якщо s – довжина шифрованого повідомлення, отриманого в результаті зашифрування m_P в СБРК D, тоді в новій схемі розшифрування ключів D' довжина такого повідомлення дорівнює ms. При цьому, розшифрувати його зможуть учасники коаліції P і тільки вони (також з цього випливає, що СБРК D і D' мають однакову стійкість).

В [12] сформульовано твердження про те, що для будь якої СБРК D і похідної пари множин (C,H), що задовільняють умові (1), ймовірність події $\left\{x^*(C,H) \notin C\right\}$ неймовірно мала, якщо тільки

$$t^2 < \frac{n}{4\log \upsilon} \tag{3}$$

(оцінки вказаної ймовірності не наводяться). Цей результат можливо значно підсилити, принаймні, в тому випадку, коли вихідна СБРК D є кодовою схемою розподілу ключів.

ТВЕРДЖЕННЯ 1. Нехай $G-(n,k,d)_q$ – код, $k \geq 2$, D – СБРК що відповідає коду G. Тоді при виконанні умови

$$t^2 < \frac{n}{n-d}. \tag{4}$$

СБРК D є t-ідентифікуючою.

Доведення. Нехай (C,H) задовільняє умові (1). Тоді з умови $H \subseteq \bigcup_{x \in C} K_x$ та нерівності $\left|H\right| \geq n$. З цього випливає, що $n \leq \left|H\right| \leq \sum_{x \in C} \left|H \cap K_x\right|$ і, отже, існує $x_0 \in C$ таке, що $\upsilon_{x_0} \geq nt^{-1}$ (значення υ_{x_0} визначається за формулою (2)).

Покажемо, що для будь якого $x \in V \setminus C$ виконується нерівність

$$\upsilon_{x_0} < nt^{-1} \tag{5}$$

звідки випливає необхідне твердження. Дійсно, $\upsilon_x = |H \cap K_x| \le \left|(\bigcup_{y \in C} K_y) \cap K_x\right| \le \sum_{y \in C} |K_y \cap K_x|$ і, оскільки $|K_y \cap K_x| \le n - c$ для будь яких $x \ne y$, тоді $\upsilon_x \le t(n-d) < nt^{-1}$ (остання нерівність виходить з умови (4)).

З цього випливає, що для будь якого $x \in V \setminus C$ виконується нерівність (5), що необхідно було довести.

НАСЛІДОК. Якщо в умові твердження G – код МДР тоді СБРК D є t-ідентифікуючою при виконанні умови:

$$t^2 < \frac{n}{k-1}. \tag{6}$$

Слід відзначити, що оцінка (6) суттєво краща оцінки (4), яка в даному випадку має вигляд $t^2 < \frac{n}{4k \log q}$.

Розглянемо СБРК D', що відповідає кодовій СБРК D та відображенню $\sigma : B' \to B$ такому, що $|\sigma^{-1}(j)| = m$ для будь якого $j \in B$.

ТВЕРДЖЕННЯ 2. В СБРК D' для будь якої пари множина (C, H), задовільняють умову (1), виконується наступна нерівність:

$$P\{x^*(C,H) \notin C\} \le q^k \exp\left\{-2n\left(\frac{N}{nt} - \frac{(n-d)t}{n \cdot m}\right)^2\right\}. \tag{7}$$

Доведення. З (1) випливає, що існує $x_0 \in C$ такий, що $\upsilon_{x_0} \ge Nt^{-1}$. У зв'язку з цим подія $\{x^*(C,H) \notin C\}$ породжує подію $\bigcup_{x \in V \setminus C} \{\upsilon_x > Nt^{-1}\}$.

Зафіксуємо $x \in V \setminus C$ та покажемо, що

$$P\{\upsilon_x > Nt^{-1}\} \le \exp\left\{-2n\left(\frac{N}{nt} - \frac{(n-d)t}{n-m}\right)^2\right\}, \tag{8}$$

звідки безпосередньо випливає нерівність (7).

Нехай $x = (x_1, \ldots, x_n)$, $C = (z_1, \ldots, z_t)$, де $z_l = (z_{l,1}, \ldots, z_{l,n})$, $l \in \overline{1,t}$, вектори x і $z_l (l \in \overline{1,t})$ є словами коду G (див. рис. 1). Для будь якого $i \in \overline{1,n}$ позначимо t_i число символів алфавіту в i-му стовпчику таблиці C, рівних x_i.

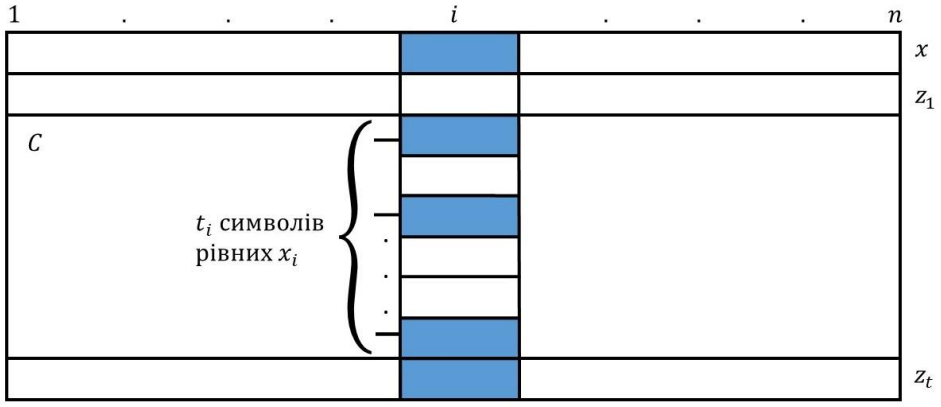

Рисунок 1 – Представлення кодових слів і частот появи символів у кожній позиції коду

Передусім зауважимо, що сума відстаней від слова x до слів $z_1,\ldots,z_t$ дорівнює $\sum_{i=1}^{n}(t-t_i)$, з однієї сторони, та більше або дорівнює $t\cdot d$ – з іншої, звідки випливає, що

$$\frac{1}{n}\sum_{i=1}^{n}t_i \le \frac{(n-d)t}{n}. \tag{9}$$

Позначимо μ_x випадкову величину, що дорівнює кількості ключів абонента x, що належать хоча б одному абоненту коаліції C. Зауважимо, що $\upsilon_x \le \mu_x$, та що μ_x є сумою n випадкових величин:

$$\mu_x = \zeta_1 + \ldots + \zeta_n, \tag{10}$$

де $\zeta_i = 1$, якщо ідентифікатор ключа абонента x, що вибирається випадково та рівноймовірно з множини $\sigma^{-1}(i,x_i)$, співпадає хоча б з одним ідентифікатором ключів абонентів $z_1,\ldots,z_t$ (які вибираються випадково і рівноймовірно із множин $\sigma^{-1}\left(i,z_{1,i}\right),\ldots,\sigma^{-1}\left(i,z_{t,i}\right)$ відповідно); $\zeta_i = 0$ – в протилежному випадку, $i \in \overline{1,n}$.

Оскільки всі ідентифікатори ключів в СБРК D' незалежні в загальному, тоді випадкові величини $\zeta_1,\ldots,\zeta_n$ в правій частині рівності (10) є незалежними. При цьому, відповідно до означення числа t_i,

$$P\{\zeta_i = 0\} = \left(\frac{m-1}{m}\right)^{t_i}, \quad i \in \overline{1,n}. \tag{11}$$

Для оцінки верхньої ймовірності $P\left\{\mu_x > Nt^{-1}\right\}$ використаємо нерівність Хеффдінга, відповідно до якого при виконанні умови $E\mu_x < Nt^{-1}$

$$P\left\{\mu_x > Nt^{-1}\right\} = P\left\{\frac{1}{n}\left(\mu_x - E\mu_x\right) > \frac{N}{nt} - \frac{E\mu_x}{n}\right\} \le \exp\left\{-2n\left(\frac{N}{nt} - \frac{E\mu_x}{n}\right)^2\right\}. \tag{12}$$

Далі, в силу (10), (11) та нерівності Бернулі $E\mu_x = \sum_{i=1}^{n}\left(1-\left(\frac{m-1}{m}\right)^{t_i}\right) \le \sum_{i=1}^{n}\left(1-\left(1-t_i m^{-1}\right)\right) = m^{-1}\sum_{i=1}^{n}t_i$, звідки, використовуючи (9), знаходимо, що $\frac{1}{n}E\mu_x \le \frac{(n-d)t}{nm}$.

Підставивши отриману оцінку в (12), робимо висновок, що при виконанні умови

$$\frac{(n-d)t}{nm} < \frac{N}{nt} \tag{13}$$

виконуються наступні нерівності:

$$P\left\{\upsilon_x > Nt^{-1}\right\} \le P\left\{\mu_x > Nt^{-1}\right\} \le \exp\left\{-2n\left(\frac{N}{nt} - \frac{(n-d)t}{nm}\right)^2\right\}.$$

Отже, нерівність (8) (при умові виконання (13)) доведено.

Таким чином, звертаючи увагу на нерівність $n \le N$ (див. (1)) можна наступним чином сформулювати отриманий результат (підправити формулювання твердження 2): при виконанні умови

$$t^2 < m\frac{n}{n-d} \tag{14}$$

для будь якої пари (C, H), що задовільняє умові (1), виконується нерівність (7).

Відзначимо, що верхня оцінка (14) в m разів вища ніж оцінка (4), що встановлює достатню умову t-ідентифікуючості вихідної (нерандомізованої) кодової СБРК D.

Висновки. У статті викладені результати синтезу алгоритму відстежування порушників на основі схем багатоадресного розподілу ключів, що застосовують кодові конструкції, які дозволяють досягати заданої точності відстежування порушників в умовах доступних (обмежених) обчислювальних ресурсів. Побудований в статті алгоритм, завдяки застосуванню оцінок Геффдінга, є t-ідентифікуючим. Отримані в статті достатні умови на параметри кодів забезпечують суттєве покращення порівняно з раніше відомими, а доведені аналітичні вирази дозволяють отримати точні нижні оцінки надійності алгоритму відстежування порушників, що, в свою чергу, може бути використане при практичній побудові рандомізованих протоколів відстежування з заданою необхідною (високою) надійністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] B. Chor, A. Fiat, and M. Naor, “Tracing Traitors”, in *Advances in Cryptology — CRYPTO ’94: 14th Ann. Int. Crypt. Conf.*, Y.G. Desmedt, Ed. Berlin, Heidelberg, Germany: Springer, 1994, pp. 257-270, doi: https://doi.org/10.1007/3-540-48658-5_25.

[2] A. Fiat, and M. Naor, “Broadcast Encryption”, in *Advances in Cryptology — CRYPTO ’93: 13th Ann. Int. Crypt. Conf.*, D.R Stinson, Ed. Berlin, Heidelberg, Germany: Springer, 1994, pp. 480-491, doi: https://doi.org/10.1007/3-540-48285-7_33.

[3] D. Boneh, and M. Franklin, “An Efficient Public Key Traitor Tracing Scheme”, in *Advances in Cryptology — CRYPTO ’99: 19th Ann. Int. Crypt. Conf.*, M. Wiener, Ed. Berlin, Heidelberg, Germany: Springer, 1999, pp. 358-371, doi: https://doi.org/10.1007/3-540-48405-1_22.

[4] K. Kurosawa, and Y. Desmedt, “Optimum Traitor Tracing and Asymmetric Schemes”, in *Advances in Cryptology — EUROCRYPT ’98*, K. Nyberg, Ed. Berlin, Heidelberg, Germany: Springer, 1998, pp. 145-157, doi: https://doi.org/10.1007/BFb0054123.

[5] G. Tardos, “Optimal Probabilistic Fingerprint Codes”, in *Proc. 35th Ann. ACM Symp. on Theory of Comp. (STOC ’03)*, New York, NY, USA: ACM, 2003, pp. 116-125, doi: https://doi.org/10.1145/779928.779941.

[6] D. Boneh, and J. Shaw, “Collusion-Secure Fingerprinting for Digital Data”, *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897-1905, 1998, doi: https://doi.org/10.1109/18.720541.

[7] S. Ling, R.C.-W. Phan, and D. Stehlé, “A Lattice-Based Traitor Tracing Scheme”, *IACR Cryptology ePrint Archive*, paper 2012/088, 2012. [Online]. Available: https://eprint.iacr.org/2012/088. Accessed on: Nov. 05, 2025.

[8] N. Attrapadung, and H. Imai, “Conjunctive Broadcast and Attribute-Based Encryption”, in *Pairing-Based Cryptography — Pairing 2009*, H. Shacham and B. Waters, Eds. Berlin, Heidelberg, Germany: Springer, 2009, pp. 248-265. doi: https://doi.org/10.1007/978-3-642-03298-1_1.

[9] P. Ananth, S. Garg, A. Sahai, and A. Srinivasan, “New Techniques for Traitor Tracing: Size $N^{1/3}$ and More from Pairings”, *IACR Cryptology ePrint Archive*, paper 2020/954, 2020. [Online]. Available: https://eprint.iacr.org/2020/954. Accessed on: Nov. 05, 2025.

[10] A. Kiayias, and Q. Tang, “How to keep a secret: leakage deterring public-key cryptosystems”, in *Proc. 2013 ACM SIGSAC Conf. on Comp. & Comm. Sec. (CCS '13)*, Berlin, Germany, pp. 943-954, 2013. Doi: https://doi.org/10.1145/2508859.2516691.

[11] A.N. Alekseichuk, and S.N. Konyushok, “Multicast key distribution schemes based on Stinson-Van Trung designs”, *Cybernetics and Systems Analysis*, vol. 43, no. 3, pp. 397-406,

2007. [Online]. Available: http://link.springer.com/article/10.1007/s10559-007-0062-6. Accessed on: Nov. 05, 2025.

[12] E. Gafni, J. Staddon, and Y.-L. Yin, “Efficient methods for integrating traceability and broadcast encryption”, in Proc*., 19th Annual International Cryptology Conference (CRYPTO '99)*, Santa Barbara, California, USA, 1999, pp. 372-387. doi: https://doi.org/10.1007/3-540-48405-1_24.

Стаття надійшла до редакції 07.10.2025.

REFERENCES

[1] B. Chor, A. Fiat, and M. Naor, “Tracing Traitors”, in *Advances in Cryptology — CRYPTO ’94: 14th Ann. Int. Crypt. Conf.*, Y.G. Desmedt, Ed. Berlin, Heidelberg, Germany: Springer, 1994, pp. 257-270, doi: https://doi.org/10.1007/3-540-48658-5_25.

[2] Fiat, and M. Naor, “Broadcast Encryption”, in *Advances in Cryptology — CRYPTO ’93: 13th Ann. Int. Crypt. Conf.*, D.R Stinson, Ed. Berlin, Heidelberg, Germany: Springer, 1994, pp. 480-491, doi: https://doi.org/10.1007/3-540-48285-7_33.

[3] D. Boneh, and M. Franklin, “An Efficient Public Key Traitor Tracing Scheme”, in *Advances in Cryptology — CRYPTO ’99: 19th Ann. Int. Crypt. Conf.*, M. Wiener, Ed. Berlin, Heidelberg, Germany: Springer, 1999, pp. 358-371, doi: https://doi.org/10.1007/3-540-48405-1_22.

[4] K. Kurosawa, and Y. Desmedt, “Optimum Traitor Tracing and Asymmetric Schemes”, in *Advances in Cryptology — EUROCRYPT ’98*, K. Nyberg, Ed. Berlin, Heidelberg, Germany: Springer, 1998, pp. 145-157, doi: https://doi.org/10.1007/BFb0054123.

[5] G. Tardos, “Optimal Probabilistic Fingerprint Codes”, in *Proc. 35th Ann. ACM Symp. on Theory of Comp. (STOC ’03)*, New York, NY, USA: ACM, 2003, pp. 116-125, doi: https://doi.org/10.1145/779928.779941.

[6] D. Boneh, and J. Shaw, “Collusion-Secure Fingerprinting for Digital Data”, *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897-1905, 1998, doi: https://doi.org/10.1109/18.720541.

[7] S. Ling, R.C.-W. Phan, and D. Stehlé, “A Lattice-Based Traitor Tracing Scheme”, *IACR Cryptology ePrint Archive*, paper 2012/088, 2012. [Online]. Available: https://eprint.iacr.org/2012/088. Accessed on: Nov. 05, 2025.

[8] N. Attrapadung, and H. Imai, “Conjunctive Broadcast and Attribute-Based Encryption”, in *Pairing-Based Cryptography — Pairing 2009*, H. Shacham and B. Waters, Eds. Berlin, Heidelberg, Germany: Springer, 2009, pp. 248-265. doi: https://doi.org/10.1007/978-3-642-03298-1_1.

[9] P. Ananth, S. Garg, A. Sahai, and A. Srinivasan, “New Techniques for Traitor Tracing: Size $N^{1/3}$ and More from Pairings”, *IACR Cryptology ePrint Archive*, paper 2020/954, 2020. [Online]. Available: https://eprint.iacr.org/2020/954. Accessed on: Nov. 05, 2025.

[10] A. Kiayias, and Q. Tang, “How to keep a secret: leakage deterring public-key cryptosystems”, in *Proc. 2013 ACM SIGSAC Conf. on Comp. & Comm. Sec. (CCS '13)*, Berlin, Germany, pp. 943-954, 2013. Doi: https://doi.org/10.1145/2508859.2516691.

[11] A.N. Alekseichuk, and S.N. Konyushok, “Multicast key distribution schemes based on Stinson-Van Trung designs”, *Cybernetics and Systems Analysis*, vol. 43, no. 3, pp. 397-406, 2007. [Online]. Available: http://link.springer.com/article/10.1007/s10559-007-0062-6. Accessed on: Nov. 05, 2025.

[12] E. Gafni, J. Staddon, and Y.-L. Yin, “Efficient methods for integrating traceability and broadcast encryption”, in Proc*., 19th Annual International Cryptology Conference (CRYPTO '99)*, Santa Barbara, California, USA, 1999, pp. 372-387. doi: https://doi.org/10.1007/3-540-48405-1_24.

VALERII ZAKUSILO,
SERHII KONIUSHOK

ALGORITHM FOR TRACKING VIOLATORS IN MULTI-ADDRESS KEY DISTRIBUTION SCHEMES

The article is devoted to the study of randomized multi-address key distribution schemes based on code constructions and their application for implementing traitor tracing schemes. A multi-address key distribution scheme is a cryptographic protocol in which a key distribution center transmits certain auxiliary information (to which only authorized users should have access) to subscribers of a communication network so that, over time, in the event of compromise of the cryptographic keys of some subscribers, whose list the key distribution center has managed to establish, other subscribers will be able to restore the shared cryptographic key, which is transmitted in encrypted form from the key distribution center via a broadcast communication channel. At the same time, subscribers whose keys have been compromised will not be able to decrypt the broadcast message. As can be seen, for such schemes to function successfully, there is a need for approaches and tools to establish a list of compromised subscribers (for different tasks, there may be a need for either a complete list of such subscribers or at least one of them). Classic traitor tracing schemes can be the basis for building such tools because they were created to identify a user or group of unscrupulous users who transferred their keys to create an array of compromised keys that can be used for malicious purposes (the so-called “violators decoder”). However, with the growing number of subscribers, the rapid development of computing resources, the creation of adaptive attacks, and increasing privacy requirements, such schemes are becoming less effective.

The approach proposed in the article aims to combine the capabilities of multi-address key distribution schemes and intruder tracking schemes while maintaining a balance between the accuracy of intruder tracking and the efficiency of available computing resources. Thanks to the use of Geffding's estimates, the algorithm constructed in the article is t-identifying, i.e., it is capable of guaranteeing the identification of at least one participant in any coalition that does not exceed t violators. The sufficient conditions given for the code parameters provide a significant improvement over the classical ones. It is demonstrated that the randomized approach preserves the stability of the system and does not degrade the security properties of the original scheme, but significantly enhances its ability to distinguish users in case of key compromise. The analytical expressions obtained in the article allow obtaining accurate lower bounds on the reliability of the traitor tracing algorithm, which, in turn, can be used in the practical construction of randomized traitor tracing protocols with a given required (high) reliability.

Keywords: cybersecurity; cyber defense; cryptography; traitor tracing; multi-address key distribution scheme.

Закусіло Валерій Олегович, аспірант, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, ORCID 0000-0001-6906-2742, zak.valera@gmail.com.

Конюшок Сергій Миколайович, кандидат технічних наук, доцент, заступник начальника інституту (з наукової роботи), Інститут спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, ORCID 0000-0003-4121-1464, 3tooth@gmail.com.

Zakusilo Valerii, postgraduate, Institute of special communication and information protection of National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute», Kyiv, Ukraine.

Koniushok Serhii, associate professor, candidate of technical sciences, deputy head of the institute (for scientific work), Institute of special communication and information protection of National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute», Kyiv, Ukraine.