КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.279293
УДК 004.056.5

Ціхоцький Микита Сергійович
асистент кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID ID: 0009-0005-8101-3536
nik.tsikhotskyi@vntu.edu.ua

Лужецький Володимир Андрійович
д.т.н., професор, завідувач кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID ID: 0000-0001-7466-7738
lva.kzi2002@gmail.com

АНАЛІЗ МЕТОДІВ РОЗПОДІЛУ СЕКРЕТУ

Анотація. Розподіл секрету — це один із ключових напрямків сучасної криптографії, який набуває все більшого значення через експоненційне зростання обсягів інформації, що передаються, зберігаються та обробляються в цифрових системах. Від соціальних мереж до медичних баз даних, інформація виступає віддзеркаленням нашої реальності у цифровому світі. Ця динаміка супроводжується численними викликами, пов'язаними із забезпеченням конфіденційності, цілісності та доступності даних, що потребують нових криптографічних підходів. Методи розподілу секрету стають важливою альтернативою традиційним методам криптографії, оскільки вони дозволяють зберігати конфіденційність, надійність і доступність інформації, розподіляючи її між кількома учасниками так, що для відновлення даних потрібна участь певної кількості сторін. Ключовими прикладами таких схем є схема Шаміра, схема Блеклі, методи на основі цифрової обробки сигналів і китайської теореми про залишки. Схема Шаміра базується на поліномах, які поділяються між учасниками, і для відновлення секрету необхідно зібрати певну кількість часток (кількість визначається заздалегідь). Схема Блеклі використовує геометричні методи, де учасники отримують координати, що дозволяють відновити секрет на основі перетину цих точок. Кожна зі схем має свої переваги та недоліки. Наприклад, схема Шаміра є ефективною з погляду простоти реалізації, але вона може вимагати великих обчислювальних ресурсів при великій кількості учасників. Схема Блеклі, навпаки, може бути більш складною в реалізації, проте зменшує обчислювальні витрати. Методи на основі цифрової обробки сигналів і китайської теореми про залишки також пропонують цікаві підходи до розподілу секрету. Алгоритми цифрової обробки сигналів дозволяють використовувати властивості сигналів для поділу інформації між учасниками, тоді як китайська теорема про залишки дозволяє розділяти секрет на основі математичних залишків від поділу числа на кілька модулів. У дослідженні представлено порівняння цих методів розподілу секрету, враховуючи різні критерії, такі як рівень безпеки, складність реалізації та вимоги до ресурсів.

Ключові слова: розподіл секрету; структура доступу; схема Шаміра; схема Блеклі; китайська теорема про залишки; алгоритми цифрової обробки сигналів.

ВСТУП

Постановка проблеми. Розподіл секрету, який є одним із розділів сучасної криптографії, бере свій витік від початкових прагнень захистити конфіденційну інформацію від небажаного доступу. Від часів робіт Аді Шаміра та Джорджа Блеклі наприкінці 1970-х років, коли було запропоновано перші формальні схеми розподілу секрету, цей напрямок переживає значний розвиток.

Сучасний інформаційний вік, що характеризується все більшою кількістю цифрових транзакцій, збільшив потребу в захищеному спільному зберіганні та доступі до даних. Водночас, традиційні методи криптографічного захисту часто можуть виявитися недостатніми перед сучасними загрозами. Отже, існує безперервна потреба в розробці нових, більш надійних методів розподілу секрету.

Сьогоднішні дослідницькі завдання в напрямку розподілу секрету спрямовані на:

1. Створення більш ефективних схем. З метою підтримки величезних обсягів даних та високошвидкісних операцій потрібні методи, що вимагають менше обчислювальних ресурсів;
2. Забезпечення універсальності. Адаптація схем розподілу секрету для різноманітних застосувань, включаючи хмарні сервіси, Інтернет речей та мобільні пристрої;
3. Забезпечення сумісності. Гармонізація з іншими криптографічними системами та протоколами забезпечення конфіденційності, цілісності та автентифікації;
4. Захист від квантових загроз. З розвитком квантової комп'ютерної техніки постає потреба в розробці схем, стійких до потенційних квантових атак.

Враховуючи динамічний характер сучасних кіберзагроз та стрімкий розвиток технологій, можна стверджувати, що розподіл секрету продовжуватиме залишатися в центрі уваги наукової спільноти. Нові методи, які будуть пропонуватися, будуть спрямовані на забезпечення вищого рівня безпеки та ефективності в умовах постійно змінюваного технологічного ландшафту.

Метою статті є дослідження існуючих методів розподілу секрету.

Об’єктом дослідження є процес розподілу секрету.

Предметом дослідження є методи та схеми розподілу секрету.

ЗАГАЛЬНИЙ ОПИС МЕТОДУ РОЗПОДІЛУ ЗОБРАЖЕННЯ

В криптографії термін «секрет» вказує на важливу інформацію, яка повинна залишатися прихованою від неавторизованих осіб [1]. Це може бути ключ для шифрування, пароль доступу, важливі документи, або як у нашому випадку зображення (в контексті даної статті надалі розглядаємо поняття секрету та зображення як взаємозамінні). В ідеалі, секрет повинен бути недоступний для тих, хто не має на це дозволу, і може бути відновлений лише тими, хто має необхідні повноваження [2]. Секрет може бути фотографією, графічним зображенням або будь-яким іншим мультимедійним вмістом.

Для розуміння процесу розподілу зображення та роботи методів, доцільно розглянути базові поняття процесу розподілу секрету.

Схема розподілу секрету (СРС) передбачає наявність дилера, який зберігає секрет. Цей дилер поширює секрет серед групи учасників (так званих користувачів або тримачів часток секрету) таким чином, щоб кожна сторона володіла часткою (або фрагментом) цього секрету. Деякі підгрупи учасників можуть відновити секрет, в той час як інші не можуть. Групи, які можуть відновити секрет, називаються кваліфікованими (або іноді уповноваженими), а інші групи називаються неуповноваженими (або іноді забороненими) [3].

Нехай $P = \{\rho_1, \dots, \rho_n\}$ є множиною учасників. Група $A_* \subseteq 2^p$ монотонно зростає якщо $A \in A_*$ та $A \subseteq B$ означає що $B \in A_*$. Це означає, що кожна супермножина з A також у A_*. Так само множина $B_* \subseteq 2^\rho$ монотонно спадає якщо для кожної множини B

у B_* також кожна підмножина B є у B_*. Монотонно зростаюча множина A_* може бути ефективно описана множиною A^-, яка складається з мінімальних елементів (множин) у A_*, тобто елементи в A_* для яких в множині A_* також немає відповідної підмножини. Так само множина B^+ складається з максимальних елементів (множин) у B_*, тобто елементи в B_* для яких у множині B_* немає відповідної підмножини.

Нехай $A_* \subseteq 2^\rho$ це множина уповноважених груп учасників і $B_* \subseteq 2^\rho$ множина неуповноважених груп. Кортеж (A_*, B_*) називається *структурою доступу* якщо $A_* \cap B_* = \emptyset$. Він називається монотонним, якщо A_* монотонно зростає та B_* монотонно спадає. Більшість структур доступу є монотонними. Хоча бувають певні ситуації коли доцільним буде використати не монотонні структури. У випадку, якщо множина $\{a, b\}$ є кваліфікованою для ініціалізації дії, тоді будь-яка супермножина також буде здатна на це. З іншого боку, якщо група яка складається з a та b є неуповноваженою, тоді учасник a (відповідно і b) є неуповноваженим.

Якщо $A_* = \emptyset$, тоді секрет залишається секретом, і ніхто не отримає частку. Коли $A_* \cup B_* = 2^\rho$, то така структура доступу називається *досконалою* і просто може бути позначена як A_* та $B_* = {A_*}^д$, доповнення до A_*.

Нехай у компанії потрібно встановити доступ до ключа, який використовується для проведення транзакцій у більшому розмірі ніж це передбачено базовими потребами. І так щоб цей доступ був розподілений між (щонайменше одним) заступником директора і одним менеджером. Допустимо що ключ s належить до K_q, де q є цілим числом. Нехай d_1, d_2 будуть заступники директора, а m_1, m_2 менеджери. Тоді ми будемо мати:

$$A_* = \begin{Bmatrix} \{d_1, m_1\}, \{d_1, m_2\}, \{d_2, m_1\}, \{d_2, m_2\}, \{d_1, m_1, m_2\}, \{d_2, m_1, m_2\}, \\ \{d_1, d_2, m_1\}, \{d_1, d_2, m_2\}, \{d_1, d_2, m_1, m_2\} \end{Bmatrix}$$

та

$$B_* = \{\emptyset, \{d_1\}, \{d_2\}, \{m_1\}, \{m_2\}, \{d_1, d_2\}, \{m_1, m_2\}\}.$$

Пара (A_*, B_*) є структурою доступу оскільки $A_* \cap B_* = \emptyset$. Ця структура доступу є монотонною і досконалою. Нехай для кожного заступника директора дано частку a (випадково обрану з K_q) і кожному менеджеру частка $s+a$. Тоді всі елементи з A_* можуть обчислити s в той час як жоден елемент B_* не здатний цього зробити.

Фактично, оскільки a вибрано випадковим чином з K_q і воно не залежить від s, частка $a+s$ рівномірно розподілена по K_q. Це означає, що $a+s$ приймає кожне значення з однаковою ймовірністю, тому $a+s$ не розкриває жодних відомостей про s. З іншого боку, група, що містить частки a і $a+s$ може обчислити ключ s шляхом віднімання частки a від частки $a+s$.

Ця схема може бути розглянута у вигляді пари (розподіл, відновлення) протоколів (або фаз).

Фаза розподілу складається з дилера P_0 для розподілу секрету s між учасниками (в нашому випадку заступники директора і менеджери, кожен отримує частку) і фаза відновлення, яка складається з учасників, які відновлюють s. Отже, учасники будь-якої множини B_* не володіють жодною інформацією про секрет s і більше того, ключ s може бути обчислений будь-якою множиною учасників $A \in A_*$. Також варто зазначити, що розмір часток відповідає розміру секрету.

Ця пара протоколів разом із двома вище згаданими властивостями реалізує ту, що прийнято називати схемою розподілу секрету на основі структури доступу.

Схема розподілу секрету, заснована на структурі доступу (A_*, B_*), є парою (розподіл, відновлення) протоколів, так що протокол розподілу відповідає за обчислення часток, які далі таємно розповсюджує дилер між учасникам та протокол відновлення,

який полягає в тому, що групи учасників намагаються реконструювати секрет на основі поєднання своїх часток. Крім того, схема повинна мати такі властивості:

- конфіденційність, учасники будь-якої множини B_* не володіють інформацією про секрет s;
- коректність, ключ s може бути обчислений будь-якою множиною учасників $A \in A_*$.

Коли $B^д = A_*$ (тобто структура доступу є досконалою), то схема розподілу секрету називається *ідеальною* [4].

Важливою характеристикою схеми розподілу секрету є *поріг* [5].

Поріг вказує на те скільки учасників або їх часток секрету потрібно, щоб відновити початковий секрет. Це важлива концепція для забезпечення безпеки та обмеження доступу до секретної інформації. Наприклад, у схемі розподілу секрету (k, n), де k — це порогова кількість учасників, а n — загальна кількість учасників, необхідно принаймні k учасників для відновлення секрету. Це означає, що менше ніж k учасників не можуть відновити секрет, зробивши систему стійкою до компрометації менше ніж k часток.

Отже визначено узагальнену схему розподілу секрету як наступний набір:

$$U = \{P, A, B, A_*, B_*, R, F\},$$

де P — скінченна множина, яка представляє всіх учасників, залучених до схеми обміну секретами $P = \{\rho_1, \dots, \rho_n\}$;

A — є підмножиною множини всіх учасників P, яка складається з уповноважених або кваліфікованих груп учасників, які, об'єднавшись, мають необхідну інформацію для відновлення секрету;

B — множина неавторизованих або некваліфікованих груп учасників схеми обміну секретами;

A_* — визначає структуру доступу (уповноважені групи учасників, які можуть колективно відновити секрет), $A_* \subseteq 2^p$;

B_* — визначає неавторизовані групи учасників, які не можуть відновити секрет, $B_* \subseteq 2^\rho$;

R — множина, яка містить функції або правила, що спрямовані на процес відновлення секрету, $R = \{r_1, r_2, \dots, r_n\}$;

F — представляє множину правил або функцій, залучених до процесу розподілу секрету, $F = \{f_1, f_2, \dots, f_n\}$, де $f: P \to S$, де S є множиною можливих часток.

ОГЛЯД МЕТОДІВ РОЗПОДІЛУ СЕКРЕТУ

Далі розглянемо основні напрямки та конкретні підходи існуючих методів розподілу секрету. А саме:

- методи на основі математичних перетворень;
- методи на основі алгоритмів цифрової обробки сигналів;
- методи на основі китайської теореми про залишки.

Методи розподілу секрету на основі **математичних перетворень** використовують математичні операції для розподілу секрету на частки так, щоб їх було можливо відновити тільки з використанням математичних перетворень або обчислень. Основні методи розподілу секрету на основі математичних перетворень:

- поліноміальні методи — у цю категорію входять методи, які використовують поліноми для розподілу секрету. Схема розподілу секрету Шаміра та схема розподілу секрету Лагранжа є прикладами таких методів.

Вони базуються на інтерполяційних поліномах та математичних властивостях поліномів для розподілу та відновлення секрету;

- геометричні методи — ці методи використовують геометричні простори та геометричні обчислення для розподілу секрету. Схема розподілу секрету Блеклі є прикладом геометричного методу, де секрет розглядається як точка в *t*-вимірному просторі, а гіперплощини використовуються для розподілу та відновлення секрету;
- деякі методи використовують числові операції та числа для розподілу секрету, такі методи називаються числовими. Схема розподілу секрету Асмута-Блума [6] та схема розподілу секрету Мінісетта використовують прості числа та комбінаторику для розподілу та відновлення секрету;
- алгебраїчні методи використовують алгебраїчні структури, такі як кільця та поля, для розподілу та відновлення секрету, використання арифметики в скінченних полях для операцій над даними;
- метод еліптичних кривих відповідно базується на використанні еліптичних кривих та їх алгебри для розподілу секрету. Точки на еліптичних кривих можуть бути використані для представлення часток секрету.

Схема розподілу Шаміра (СРШ) є ідеальною та досконалою (*k, n*) — пороговою схемою на основі поліноміальної інтерполяції над скінченними полями [1]. Схема використовує теорему про інтерполяцію Лагранжа, зокрема те, що *k* точок на поліномі однозначно визначає поліном степені, меншої або рівної *k* -1. Наприклад, 2 точки достатньо, щоб визначити лінію, 3 точки достатньо, щоб визначити параболу, 4 точки, щоб визначити кубічну криву і так далі.

У такій схемі, задачею розділення секрету *S* на *n* частин даних $S_1, \dots, S_n$ (відомі як шари) таким чином, щоб:

1. Знання будь-яких *k* або більше шарів S_i робить S обчислюваним. Тобто весь секрет S можна реконструювати з будь-якої комбінації шарів *k*;
2. Знання будь-яких *k* -1 або менша кількість шарів S_i залишає *S* повністю невизначеною в тому сенсі, що можливі значення для *S* залишаються такими ж вірогідними, якщо знати до *k* -1 шарів, як і з інформацією про шари. Секрет *S* не може бути реконструйований з менш ніж *k* шарів.

Якщо *n* = *k*, тоді всі шари будуть необхідні для реконструкції секрету *S*.

Припустимо що секрет *S* може бути представлений як елемент a_0 скінченного поля *GF(q)* де *q* є більшим ніж кількість згенерованих шарів *n*. Випадковим чином обираються елементи *k* -1, $a_1, \dots, a_{k-1}$, з *GF(q)* та будується поліном:

$$f(x) = a_0 + a_{01}x + a_2x^2 + a_3x^3 + \cdots + a_{k-1}x^{k-1} \quad (1)$$

Обчислюються будь-які з *n* точок на кривій, наприклад, набір *i* = 1, … , *n* щоб знайти точки *(i, f(i))*. Кожному учаснику надається точка (ненульовий вхід до полінома та відповідний вихід). Дано будь-яку підмножину *k* цих пар, a_0 може бути отримана за допомогою інтерполяції, з однією можливою для цього формулою:

$$a_0 = f(0) = \sum_{j=0}^{k-1} y_i \prod_{\substack{m=0 \\ m \neq j}}^{k-1} \frac{x_m}{x_m - x_j}, \quad (2)$$

де список точок полінома задається як пара *k* у формі (x_i, y_i).

СРШ має багато переваг, але також має недоліки, які означають, що вона не підходить для певних задач.

До переваг відносяться:

– схема є математично обґрунтованою та забезпечує високий рівень криптографічної безпеки;

- розмір кожної частки не перевищує розмір вихідних даних;
- для будь-якого заданого порогу спільні ресурси можна динамічно додавати або видаляти, не впливаючи на існуючі спільні ресурси;
- безпеку можна підвищити без зміни секрету, але час від часу змінюючи поліном (зберігаючи той самий вільний елемент) і створюючи новий спільний ресурс для кожного з учасників;
- у структурованих організаціях, де існує ієрархічна система, можна використовувати різні вагові коефіцієнти для кожного учасника залежно від його ролі та відповідальності. Наприклад, якщо встановлено порогове значення 3, президент може мати доступ до сейфу, використовуючи три частки, видані самому собі. У той же час, троє секретарів можуть мати по одній частці секрету, і кожен з них повинен поєднати свою частку з іншими, щоб відкрити сейф. Така система дозволяє раціонально розподіляти доступ до секретів у відповідності з ієрархією та внутрішньою організацією.

Недоліками є:

- немає перевіреного спільного доступу до секрету. Під час процесу повторного складання спільного секрету СРШ не надає можливості перевірити правильність кожного спільної частки, яка використовується. Перевірений таємний обмін має на меті переконатися, що учасники є чесними та не подають фальшиві частки;
- однією з найбільш вразливих точок у процесі розподілу секрету є єдина точка відмови. Це означає, що секрет спочатку зберігається в одному місці, потім розбивається на частки для розподілу, і знову збирається в одному місці для відновлення. Такі точки атаки стають дуже вразливими, оскільки зловмисники можуть сконцентрувати свої зусилля на зламі саме цих моментів у процесі роботи з секретом.

Далі розглянемо схему розподілу секрету, запропоновану **Блеклі** [7].

У цьому методі особа, яка володіє секретом, розподіляє ключ або секрет серед учасників, при цьому кожен учасник має свою власну частину загального секрету. Ключ може бути розкритий, коли певна кількість учасників об'єднуються і діляться своєю інформацією. Блеклі використовував геометричний підхід для вирішення цієї проблеми, розглядаючи секрет як точку у t-вимірному просторі. У цьому t-вимірному просторі перетин гіперплощин в одній точці приводить до відновлення секретного ключа. Коефіцієнти різних гіперплощин складають відповідні частки, роблячи цю схему схожою на схему Шаміра.

У підході Блеклі як секрет, так і частки можна представити у вигляді лінійної системи, позначеної як $C_x = y$, де матриця C і вектор y відповідають рівнянням гіперплощин. Метод Блеклі використовує геометричні принципи для розподілу секрету. У цьому методі секретний ключ розглядається як точка у t-вимірному просторі, а саме як точка перетину всіх гіперплощин. Афінні гіперплощини в цьому просторі представляють індивідуальні частки секрету. Схему розподілу Блеклі можна виразити як лінійну систему $C_x \ mod \ p = y$, де матриця C повного рангу відіграє критичну роль.

Для подальшого уточнення розглянемо два основні поняття в цьому підході: розподіл та відновлення. На рис. 1 зображено три різних гіперплощини у тривимірному просторі, кожна з яких представляє різних учасників згідно з визначенням.

Як показано на рис. 2, перетин трьох гіперплощин визначає лінію, а перетин двох гіперплощин породжує точку тривимірному просторі. Основна ідея полягає в тому, що дві непаралельні лінії у одній площині перетинаються у точці, так само як і три

ISSN 2663 - 4023

непаралельні гіперплощини в просторі перетинаються у конкретній точці. Загалом, будь-які *t* непаралельні (*t*-1)-вимірній гіперплощині перетинаються у конкретній точці. Секрет може бути закодований як будь-яка окрема координата цього перетину. Якщо ключ закодовано з використанням усіх координат, то інсайдер отримає інформацію про ключ, оскільки він знає, що точка повинна лежати на його площині. Якщо інсайдер отримує доступ до більшої інформації про інших, то безпека системи порушується.

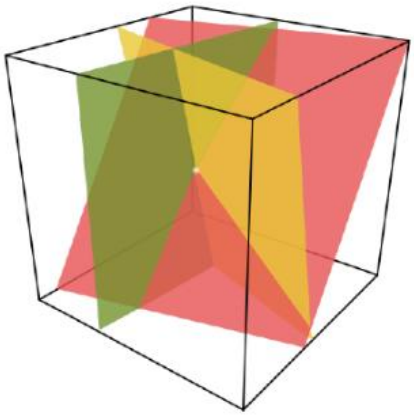

Рис. 1. Три різні гіперплощини

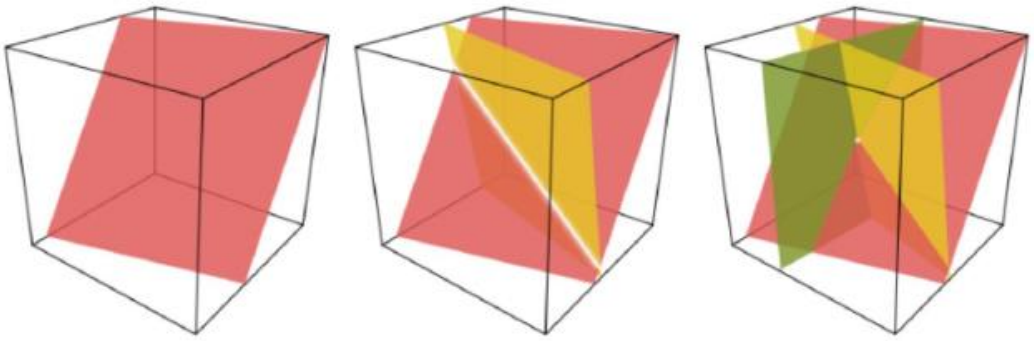

Рис. 2. *Перетин різних гіперплощин*

Далі детально опишемо процес розподілу секрету між учасниками. Це завдання може виконати дилер.

1. Обирається просте число *(p)*;
2. Створюється точка, використовуючи секретну інформацію x_0;
3. Обираються випадкові значення для осей Y_0 і Z_0 за модулем *p*;
4. Використовуючи попередні значення, знаходиться точка перетину $Q(x_0, y_0 z_0)$;
5. Далі обираються значення для *a* та *b* за модулем *p* і знаходиться значення *c* для конкретної гіперплощини так, щоб:
$$c = z_0 - ax_0 - by_0 (mod\ p) \quad (3)$$
6. На основі значень *a, b* та *c*, визначається гіперплощина для кожного з учасників:
$$z = ax + by + c (mod\ p) \quad (4)$$

Тепер у кожного є конкретна гіперплощина. Наприклад, створення гіперплощин для п'яти учасників приведе до:

$$\begin{aligned} a_1x + b_1y - z = -c_1(mod\ p) \\ a_2x + b_2y - z = -c_2(mod\ p) \\ a_3x + b_3y - z = -c_3(mod\ p) \\ a_4x + b_4y - z = -c_4(mod\ p) \\ a_5x + b_5y - z = -c_5(mod\ p), \end{aligned} \quad (5)$$

які можна узагальнити як:

$$a_ix + b_iy - z = -c_i(mod\ p)\ , \quad (6)$$

де $1 \le i \le 5$.

Отже, якщо вибрати лише трьох учасників із п'яти осіб, можна знайти секретний ключ, який є значенням x_0 у цьому конкретному прикладі. Знаходячи розв'язок для наступного рівняння, буде знайдено значення для секретного ключа. Поки визначник матриці є відмінним від нуля за модулем p, матрицю можна інвертувати, а секрет можна знайти.

$$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} mod\ (p) \quad (7)$$

Основними недоліками схеми Блеклі є:

- висока складність відновлення секрету, при великій кількості учасників процес відновлення секрету може бути дуже складним і витратним;
- відомість порогових значень, в схемі Блеклі порогові значення (кількість часток, необхідних для відновлення секрету) відомі усім учасникам. Це може збільшити ризик компрометації секрету;
- слабка стійкість до атак, у разі втрати навіть однієї частки секрету зловмисники можуть легко відновити секрет, якщо їм відомі порогові значення;
- потенційна складність масштабування, збільшення кількості учасників може призвести до збільшення складності процесу розподілу та відновлення секрету.

Через ці недоліки підхід Блеклі є менш популярним порівняно зі схема Шаміра. Однак дослідники почали використовувати підхід розподілу секрету, заснований на геометрії Блеклі, у сфері обміну секретними зображеннями. Улутас та ін. [8] представили вдосконалену схему для розподілу секретних зображень, яка використовує метод розподілу секрету Блеклі з іншим методом для обміну секретом і створення значимих спільних ресурсів. Крім того, Бозкурт та ін. [9] пояснили перший пороговий підхід підпису RSA за допомогою схеми Блеклі.

Методи розподілу секрету на основі алгоритмів цифрової обробки сигналів

Дані методи використовують різні сигнали або сигнальні процеси для розподілу секретної інформації. Основна ідея полягає в тому, щоб перетворити секретну інформацію у сигнал або обробити існуючий сигнал таким чином, щоб він містив частину секрету, а потім розподілити цей сигнал серед учасників так, щоб вони могли відновити секрет за певних умов. Для реалізації цього підходу розглядаються:

1. Методи, що використовують перетворення Фур'є [10].

Перетворення Фур'є є математичним інструментом, призначеним для перетворення сигналів між часовим і частотним просторами. У контексті

розподілу секрету, секрет може бути перетворений в частотний простір, де його частотні компоненти розподіляються серед учасників.

2. Методи, що використовують фільтрацію [11].

Використання фільтрації дозволяє виділити специфічні компоненти сигналу. Для розподілу секрету може використовуватися фільтрація для виділення чи приховування певних аспектів інформації перед її розподілом.

3. Методи, що використовують кореляцію та обробку сигналів [12].

Кореляція може допомогти визначити зв'язки між різними частками секрету. Використовуючи кореляцію та інші методи обробки сигналів, можна створювати системи розподілу секрету, які вимагають координованої дії між учасниками для відновлення секрету.

4. Методи, що використовують цифрову обробку зображень [13].

Ці методи концентруються на зображеннях як сигналах. Застосування методів обробки зображень передбачає використання операцій: маскування, стеганографічного перетворення або інші види маніпуляцій з пікселями для кодування та розподілу секрету.

5. Методи, що використовують перетворення сигналу [14].

Перетворення сигналу може включати різні математичні та статистичні операції. У контексті розподілу секрету, секрет може бути перетворений або модифікований з метою його подальшого розподілу та захисту.

Більшість методів обробки одновимірних сигналів (наприклад, медіанний фільтр) можуть застосовуватись і до двомірних сигналів, якими є зображення. Деякі з цих одновимірних методів значно ускладняються з переходом до двовимірних сигналів. Обробка зображень вносить сюди кілька нових понять, таких як зв'язність і ротаційна інваріантність [15], які мають сенс тільки для двовимірних сигналів. У обробці сигналів широко використовуються перетворення Фур'є, а також Вейвлет-перетворення [16] і фільтр Габора [17].

Для прикладу більш детально розглянемо процес розподілу секрету використовуючи перетворення Фур'є:

1. Спочатку секрет M представляється як набір коефіцієнтів полінома або вектора;
2. Виконується дискретне перетворення Фур'є на цей вектор, отримуючи комплексні частоти F;
3. Замість розподілу самого секрету, розподіляються частоти F, отримані в результаті перетворення;
4. Кожна частка представляє собою частину спектру перетворення;
5. Кожна частка S_i представляє собою певну частину спектру перетворення Фур'є. Це може бути окремий комплексний коефіцієнт або набір коефіцієнтів;
6. Частки S_i передаються учасникам P_i. Кожен учасник отримує одну або кілька часток;
7. Для відновлення секрету необхідно зібрати достатню кількість часток S_i;
8. Зібрані частки використовуються для зворотного дискретного перетворення Фур'є, що дозволяє відновити оригінальний вектор або поліном;
9. Якщо кількість часток недостатня, відновлення секрету буде неможливим.

Розподіл секретного вмісту зображень з використанням перетворення Фур'є має такі переваги:

- висока частотність сигналу, перетворення Фур'є дозволяє розкласти сигнал на компоненти різних частот, що може полегшити обробку та аналіз сигналу;
- ефективність при обробці сигналів, завдяки швидким алгоритмам, таким як швидке перетворення Фур'є (FFT), обчислення Фур'є можуть бути виконані дуже швидко, що важливо при обробці великих обсягів даних;
- збереження інформації, перетворення Фур'є дозволяє зберігати інформацію про частотну структуру сигналу, яка може бути важливою при розподілі секрету.

Водночас даному методу розподілу секрету притаманні такі недоліки:

- чутливість до шуму, перетворення Фур'є може бути чутливим до шуму в сигналі, що може призводити до втрати інформації під час розподілу секрету;
- обсяг даних, результатом перетворення Фур'є можуть бути великими обсягами даних, що вимагає більше ресурсів для зберігання та передачі;
- для реалізації схеми необхідно використовувати складні математичні операції з комплексними числами.

Методи розподілу секрету на основі китайської теореми про залишки

Китайська теорема про залишки (КТЗ) стверджує, що якщо відомі залишки від цілочисельного ділення числа n на кілька інших чисел, то можна унікально визначити залишок ділення n на добуток цих чисел, за умови, що дільники є попарно взаємно простими (жодні два дільники не мають спільних множників, крім 1).

Схема розподілу секрету на основі КТЗ полягає у відновленні секрету S з набору часткової інформації, яка міститься в кожному з розданих часток [18]. Китайська теорема про залишки стверджує, що для даної системи одночасних конгруентних рівнянь розв'язок єдиний в деякому кільці Z/nZ, де $n>0$ при відповідних умовах для конгруентностей. Схема розподілу секрету може використовувати КТЗ для створення часток, які представлені у конгруентних рівняннях. Секрет може бути відновлений шляхом вирішення системи конгруентних рівнянь, щоб отримати єдиний розв'язок, який буде секретом, що відновлюється.

При $k \geq 2, m_1, \dots, m_k \geq 2,$ та $b_1, \dots, b_k \in Z$. Система конгруентностей:

$$\begin{cases} x \equiv b_1 mod\ m_1 \\ \quad . \\ \quad . \\ x \equiv b_k mod\ m_k \end{cases} \tag{8}$$

має рішення для Z (цілі числа) тоді і лише тоді, коли $b_i \equiv b_j \bmod (m_i, m_j)$ для всіх $1 \leq i, j \leq k$, де (m_i, m_j) позначає найбільший спільний дільник m_i та m_j. Крім того, за цих умов, система має єдиний розв'язок в Z/nZ, де $n = [m_1, \dots, m_k]$, що позначає найменше спільне кратне $m_1, \dots, m_k$.

Оскільки китайська теорема про залишки надає нам можливість унікально визначити число S за модулем k взаємно простих цілих чисел $m_1, m_2, \dots, m_k$ з умовою, що $S < \prod(mi)$ та $S \geq \prod(mi)$, то ідея полягає в створенні схеми, яка дозволить визначити секрет S за будь-яких k часток (в цьому випадку залишку S модуль кожного з чисел m_i), але не розкриє секрет за менше, ніж k таких часток.

Таким чином, завдяки китайській теоремі про залишки, можна унікально визначити S з будь-якого набору k або більше часток, але не менше, ніж k. Отже, отримуємо так звану порогову структуру доступу.

Умову щодо S також можна розглядати як:

$$\prod_{i=2-k+2}^{n} m_i < S < \prod_{i=1}^{k} m_i \,, \qquad (9)$$

де i належить відрізку $[n\text{-}k\text{+}2, n]$, і k належить відрізку $[1, k]$.

Порогові схеми обміну секретами, засновані на китайській теоремі про залишки, були розроблені Міньоттом [10] та Асмут-Блумом [6]. Вони використовують спеціальні послідовності цілих чисел разом із КТЗ.

Порогова схема розподілу секрету Міньотта [19] використовує, разом із китайською теоремою про залишки, спеціальні послідовності цілих чисел, які називаються (k,n)-послідовностями Міньотта. Ці послідовності складаються з n цілих чисел, які є попарно взаємно простими, і такими, що добуток найменших k з них більший, ніж добуток k-1 найбільших чисел. Ця умова є вирішальною, оскільки схема побудована на виборі секрету як цілого числа між двома добутками, і ця умова гарантує, що для повного відновлення секрету потрібно щонайменше k часток, незалежно від того, як вони вибираються.

Метод розподілу секрету Асмут-Блума [6] — це порогова схема розподілу секретів, що використовує китайську теорему про залишки.

Для реалізації цього методу спочатку обираються n попарно взаємно простих чисел. Ці числа вибрані таким чином, що добуток будь-яких k-1 з них завжди менший за секрет S, а добуток будь-яких k з них — більший. Кожному учаснику відповідає частка секрету, яка є залишком від ділення S на відповідне число. Якщо k учасників об'єднають свої частки, вони можуть використовувати китайську теорему про залишки для відновлення первісного секрету S. Ця схема забезпечує високий рівень безпеки завдяки використанню математичних властивостей взаємно простих чисел.

Результати порівняльного аналізу розглянутих методів розподілу секрету наведено у табл. 1. Тут методи порівнюються на основі таких параметрів як кількість часток k/n, безпека, розмір часток, складність алгоритму та тип розподілу.

Таблиця 1

Результати порівняльного аналізу методів розподілу секрету

Автор / Параметри	**Шамір**	**Блеклі**	**Мінісетт**	**Міньотт**	**Асмут та Блум**
Кількість часток k/n	Визначається користувачем	Визначається користувачем	Визначається користувачем	Визначається користувачем	Визначається користувачем
Безпека	Висока	Середні	Середній	Висока	Висока
Розмір часток	Такий самий, як секрет	Такий самий, як секрет	Збільшений в порівнянні з секретом	Такий самий, як секрет	Збільшений в порівнянні з секретом
Автор / Параметри	**Шамір**	**Блеклі**	**Мінісетт**	**Міньотт**	**Асмут та Блум**
Складність алгоритму	Висока	Висока	Помірна	Висока	Помірна
Тип розподілу	Поліноміальна інтерполяція	На основі векторного простору	Використання матриць	На основі КТЗ	На основі КТЗ
Недоліки	Високі вимоги до обчислювальних ресурсів при великій кількості учасників	Складність реалізації, потенційні уразливості	Уразливий до атак на проміжні результати	Складність реалізації, залежність від вибору модулів	Вразливий до слабких модулів

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

За результатами проведеного аналізу існуючих методів розподілу секрету сформульовано їх основні переваги та недоліки.

Схема Шаміра вимагає великої обчислювальної потужності при обробці великих обсягів інформації. Методи на основі перетворень Фур'є можуть бути обчислювально витратними та мають обмеження щодо обробки невеликих деталей у зображенні. Схеми на основі китайської теореми про залишки також мають свої складнощі в виборі параметрів та побудові спеціальних послідовностей.

Виявлені недоліки та обмеження існуючих методів розподілу секрету показують, в яких напрямках потрібно вдосконалювати ці методи. Удосконалені методи повинні бути ефективними, безпечними та враховувати специфіку даних, з якими вони працюють. Ефективність має розглядатися з точки зору зменшення обчислювальної складності розподілення і відновлення секрету, можливості простого масштабування схеми та вибору параметрів *k* та *n*.

Використання методів розподілу секрету може бути певною альтернативою традиційним методам криптографії в таких сферах застосування, як військова справа, медицина, фінанси та інші.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shamir, A. (1979). *How to share a secret. Communications of the ACM, 22(11).* 612–613. https://doi.org/10.1145/359168.359176
2. Naor, M., & Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. *Security Protocols,* 197–202. https://doi.org/10.1007/3-540-62494-5_18
3. Liu, J., Mesnager, S., & Chen, L. (2016). Secret Sharing Schemes with General Access Structures. *Information Security and Cryptology,* 341–360. https://doi.org/10.1007/978-3-319-38898-4_20
4. Brickell, E. F. (2001). Some Ideal Secret Sharing Schemes. *Lecture Notes in Computer Science,* 468–475. https://doi.org/10.1007/3-540-46885-4_45
5. Iwamoto, M., Yamamoto, H., & Ogawa, H. (2007). Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes with General Access Structures. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E90-A(1),* 101–112. https://doi.org/10.1093/ietfec/e90-a.1.101
6. Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory, 29(2),* 208–210. https://doi.org/10.1109/tit.1983.1056651
7. Blakley, G. R. (1979). Safeguarding cryptographic keys. *1979 International Workshop on Managing Requirements Knowledge.* https://doi.org/10.1109/mark.1979.8817296
8. Ulutas, M. (2010). Meaningful share generation for increased number of secrets in visual secret-sharing scheme. *Mathematical problems in engineering, 2010,* 1–18. https://doi.org/10.1155/2010/593236
9. Bozkurt, İ. N., Kaya, K., & Selçuk, A. A. (2009). Practical threshold signatures with linear secret sharing schemes. *Progress in cryptology – AFRICACRYPT 2009,* 167–178. https://doi.org/10.1007/978-3-642-02384-2_11
10. Ohsawa, T., Kurokawa, N., & Koshiba, T. (2017). Function secret sharing using fourier basis. *Advances in network-based information systems. Cham,* 865–875. https://doi.org/10.1007/978-3-319-65521-5_78
11. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). Applications and properties. *Digital watermarking and steganography,* 15–59. https://doi.org/10.1016/b978-012372585-1.50005-x
12. Poor, H. V. (1994). *Introduction to signal detection and estimation.* Springer-Verlag.
13. Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscale images. *MM&Sec '01: Proceedings of the 2001 workshop on Multimedia and security: new challenges,* 27–30. https://doi.org/10.1145/1232454.1232466
14. Zhang, X., & Wang, S. (2009). Fragile watermarking scheme using a hierarchical mechanism. *Signal processing, 89(4),* 675–679. https://doi.org/10.1016/j.sigpro.2008.10.001
15. Gonzalez, R. C. (2014). *Digital image processing 3rd edition (paperback).* PE.

16. Akansu, A. N., Serdijn, W. A., & Selesnick, I. W. (2010). Emerging applications of wavelets: a review. *Physical communication, 3(1),* 1–18. https://doi.org/10.1016/j.phycom.2009.07.001
17. *Gabor analysis and algorithms: theory and applications*. (1998). Boston: Birkhäuser.
18. Iftene, S. (2007). General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic notes in theoretical computer science, 186,* 67–84. https://doi.org/10.1016/j.entcs.2007.01.065
19. Mignotte, M. (2000). How to share a secret. *Cryptography*, 371–375. https://doi.org/10.1007/3-540-39466-4_27

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Mykyta Tsikhotskyi
Assistant of the Department of Information Protection
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID: 0009-0005-8101-3536
nik.tsikhotskyi@vntu.edu.ua

Volodymyr Luzhetskyi
Ph.D., Professor, Head of the Information Protection Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID ID: 0000-0001-7466-7738
lva.kzi2002@gmail.com

ANALYSIS OF SECRET DISTRIBUTION METHODS

Abstract. Secret distribution is one of the key areas of modern cryptography, which is becoming increasingly important due to the exponential growth of information transmitted, stored, and processed in digital systems. From social networks to medical databases, information is a reflection of our reality in the digital world. This dynamic is accompanied by numerous challenges related to ensuring the confidentiality, integrity, and availability of data, requiring new cryptographic approaches. Secret sharing methods are becoming an important alternative to traditional cryptography methods, as they allow for the confidentiality, reliability, and availability of information by distributing it among multiple participants so that data recovery requires the participation of a certain number of parties. Key examples of such schemes include the Shamir scheme, the Blackley scheme, methods based on digital signal processing, and the Chinese residual theorem. Shamir's scheme is based on polynomials that are shared among the participants, and to recover the secret, a certain number of shares must be collected (the number is determined in advance). The Blackley scheme uses geometric methods, where participants receive coordinates that allow them to recover the secret based on the intersection of these points. Each of the schemes has its advantages and disadvantages. For example, Shamir's scheme is efficient in terms of ease of implementation, but it can require large computing resources with a large number of participants. The Blackley scheme, on the contrary, can be more complex to implement, but reduces computational costs. Methods based on digital signal processing and the Chinese residual theorem also offer interesting approaches to secret distribution. Digital signal processing algorithms allow using the properties of signals to divide information between participants, while the Chinese residual theorem allows sharing a secret based on the mathematical residuals from dividing a number into several modules. The study presents a comparison of these secret sharing methods, considering various criteria such as security level, implementation complexity, and resource requirements.

Keywords: secret distribution; access structure; Shamir scheme; Blackley scheme; Chinese remainder theorem; digital signal processing algorithms.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shamir, A. (1979). *How to share a secret. Communications of the ACM, 22(11).* 612–613. https://doi.org/10.1145/359168.359176
2. Naor, M., & Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. *Security Protocols,* 197–202. https://doi.org/10.1007/3-540-62494-5_18
3. Liu, J., Mesnager, S., & Chen, L. (2016). Secret Sharing Schemes with General Access Structures. *Information Security and Cryptology*, 341–360. https://doi.org/10.1007/978-3-319-38898-4_20
4. Brickell, E. F. (2001). Some Ideal Secret Sharing Schemes. *Lecture Notes in Computer Science*, 468–475. https://doi.org/10.1007/3-540-46885-4_45
5. Iwamoto, M., Yamamoto, H., & Ogawa, H. (2007). Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes with General Access Structures. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E90-A(1),* 101–112. https://doi.org/10.1093/ietfec/e90-a.1.101

6. Asmuth, C., & Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transactions on Information Theory, 29(2),* 208–210. https://doi.org/10.1109/tit.1983.1056651
7. Blakley, G. R. (1979). Safeguarding cryptographic keys. *1979 International Workshop on Managing Requirements Knowledge.* https://doi.org/10.1109/mark.1979.8817296
8. Ulutas, M. (2010). Meaningful share generation for increased number of secrets in visual secret-sharing scheme. *Mathematical problems in engineering, 2010,* 1–18. https://doi.org/10.1155/2010/593236
9. Bozkurt, İ. N., Kaya, K., & Selçuk, A. A. (2009). Practical threshold signatures with linear secret sharing schemes. *Progress in cryptology – AFRICACRYPT 2009,* 167–178. https://doi.org/10.1007/978-3-642-02384-2_11
10. Ohsawa, T., Kurokawa, N., & Koshiba, T. (2017). Function secret sharing using fourier basis. *Advances in network-based information systems. Cham,* 865–875. https://doi.org/10.1007/978-3-319-65521-5_78
11. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). Applications and properties. *Digital watermarking and steganography,* 15–59. https://doi.org/10.1016/b978-012372585-1.50005-x
12. Poor, H. V. (1994). *Introduction to signal detection and estimation.* Springer-Verlag.
13. Fridrich, J., Goljan, M., & Du, R. (2001). Reliable detection of LSB steganography in color and grayscale images. *MM&Sec '01: Proceedings of the 2001 workshop on Multimedia and security: new challenges,* 27–30. https://doi.org/10.1145/1232454.1232466
14. Zhang, X., & Wang, S. (2009). Fragile watermarking scheme using a hierarchical mechanism. *Signal processing, 89(4),* 675–679. https://doi.org/10.1016/j.sigpro.2008.10.001
15. Gonzalez, R. C. (2014). *Digital image processing 3rd edition (paperback).* PE.
16. Akansu, A. N., Serdijn, W. A., & Selesnick, I. W. (2010). Emerging applications of wavelets: a review. *Physical communication, 3(1),* 1–18. https://doi.org/10.1016/j.phycom.2009.07.001
17. *Gabor analysis and algorithms: theory and applications*. (1998). Boston: Birkhäuser.
18. Iftene, S. (2007). General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic notes in theoretical computer science, 186,* 67–84. https://doi.org/10.1016/j.entcs.2007.01.065
19. Mignotte, M. (2000). How to share a secret. *Cryptography,* 371–375. https://doi.org/10.1007/3-540-39466-4_27