НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт за темою

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ РЕАЛІЗАЦІЇ РОЗДІЛЕННЯ СЕКРЕТУ ЗА ДОПОМОГОЮ РІЗНИХ АСИМЕТРИЧНИХ АЛГОРИТМІВ

Виконали студенти
групи ФІ-32мн
Баєвський Констянтин,
Шифрін Денис,
Кріпака Ілля

Київ — 2023

ЗМІСТ

ВСТУП

0.1 Мета практикуму

Дослідити можливість реалізації розділення секрету за допомогою різних асиметричних алгоритмів (не менше як двох) та порівняти їх ефективність за обраним критерієм.

0.1.1 Постановка задачі та варіант

Треба виконати	**Зроблено**
Дослідити існуючі схеми розділення секрету	✓
Дослідити схеми розділення в різних асиметричних алгоритмах	✓
Порівняти їх ефективність за обраним критерієм	✓

0.2 Хід роботи/Опис труднощів

На початку роботи над практикумами вибрати варіант 1А, та далі продовжували роботу над ними. Згідно вибраного варіанту у даній роботі буде розглянуто схеми розділення секрету в різних асиметричних алгоритмах. Під час виконання звіту не виникло ніяких серйозних проблем.

1 РОЗПОДІЛ СЕКРЕТУ

Розділення секрету (англ. *secret sharing*) [1] — це спосіб безпечного розповсюдження фрагментів важливої приватної інформації серед розподіленої мережі або групи, що робить такі схеми особливо корисними для захисту дуже чутливої інформації, наприклад, приватних криптографічних ключів або біометричних даних.

Розділення секрету працює шляхом поділу приватної інформації на менші частини – або частки – і подальшого розповсюдження цих часток серед групи або мережі.

Кожен окремий ресурс марний сам по собі, але коли всі ресурси зібрані разом, вони відновлюють початковий секрет.

1.1 Існуючі схеми

Існуючі схеми мають дві складові: розподіл і відновлення секрету. До поділу відноситься формування частин секрету і розподіл їх між членами групи, що дозволяє розділити відповідальність за секрет між її учасниками. Зворотна схема повинна забезпечити його відновлення за умови доступності його зберігачів у деякій необхідній кількості.

Схеми поділу секрету застосовуються у випадках, коли існує значна ймовірність компрометації одного або декількох зберігачів секрету, але ймовірність недобросовісної змови значної частини учасників вважається мізерно малою [2].

Приклад розподілу секрету:

Уявіть, що у вас є мільйон доларів, який ви зберігаєте на банківському рахунку, і для доступу до нього ви використовуєте пароль: secret. Ви могли б розділити його на частини і розіслати по одному листу шістьом довіреним акціонерам. Єдиною інформацією, яку матиме кожен акціонер, є лист, який

він тримає на руках, що фактично робить його акції марними.

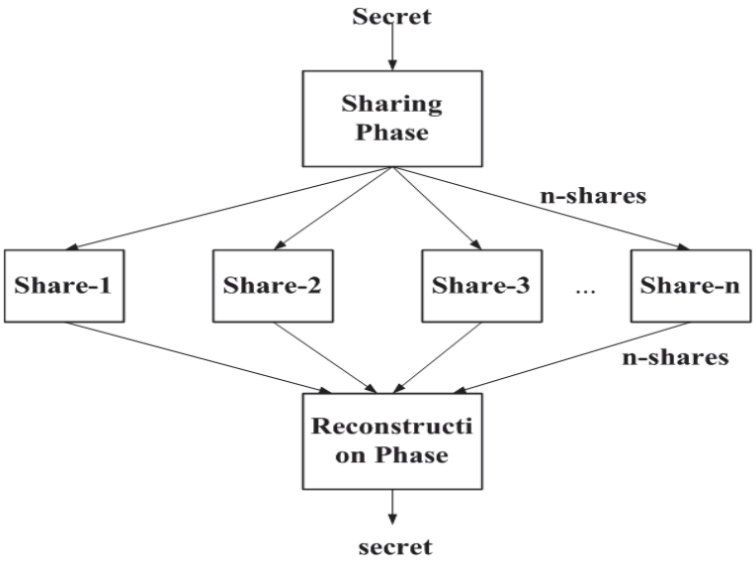

Рисунок 1.1 – Звичайна схема розподілу секрету

1.1.1 Ієрархічні схеми розподілу секрету

Схеми розподілу секрету також можуть бути ієрархічними, залежно від того, як розподіляються частки секрету. Це дозволяє власнику секрету розподіляти частки залежно від того, наскільки акціонери йому довіряють.

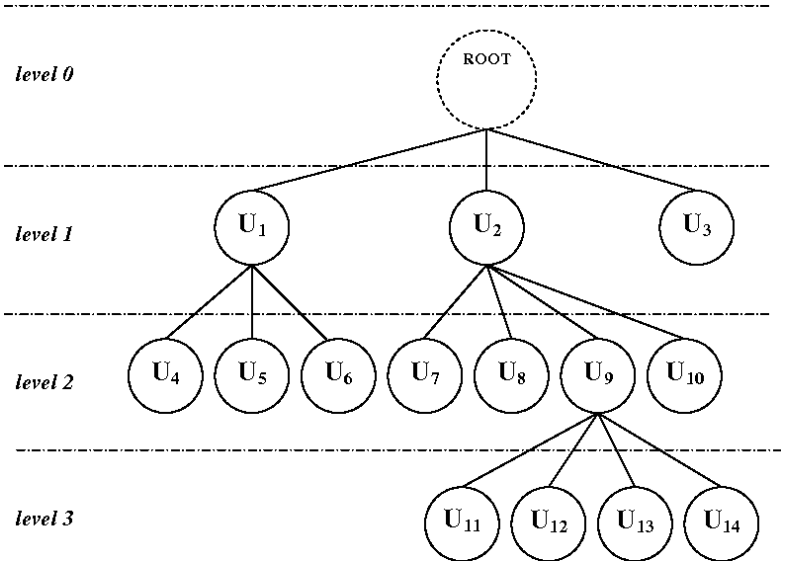

Рисунок 1.2 – Ієрархічна схема розподілу секрету

Приклад ієрархічної схеми:

Припустимо, ви хочете безпечно зберігати свій приватний ключ, який ви використовували для доступу до свого криптовалютного гаманця. Закриті ключі використовуються для переказу криптовалюти з однієї адреси на іншу. Вони складаються з послідовності випадкових і унікальних чисел і надаються користувачам під час відкриття гаманця.

По-перше, ви не захочете давати комусь всю послідовність, тому, скажімо, розділите ключ на вісім частин. Потім ви розподіляєте копії цих частин між найближчими друзями та членами сім'ї, яким ви довіряєте.

Ви можете віддати по вісім частин кожному з батьків, яким ви беззаперечно довіряєте, по чотири частини брату і сестрі, яким ви довіряєте здебільшого, і по одній частині восьми друзям, яким ви довіряєте в деякій мірі. Така ієрархічна схема розподілу дозволяє власникам розподіляти частки секрету залежно від того, наскільки вони довіряють своїм акціонерам.

1.1.2 Схеми розподілу секрету без довіри

У більшості схем, в яких немає довіри між власником секрету та акціонерами, впроваджується додатковий рівень шифрування для забезпечення додаткової конфіденційності та безпеки. Це дозволяє розподіляти частки серед мережі або групи, які невідомі власнику секрету.

Приклад схеми без довіри:

Припустимо, що кожен акціонер володіє лише випадковими числами: 19, 5, 3, 18, 5, 20.

При шифруванні, коли всі окремі частки (числа) зібрані разом, вони все одно потребують ключа-дешифрувальника, щоб розкрити секрет (літери), які вони представляють в алфавіті.

Цей важливий крок захищає приватну інформацію від організованих атак; навіть якщо кожен акціонер вступить у змову, щоб відтворити

оригінальний секрет, він не зможе нічого дізнатися про цей секрет, оскільки оригінальний секрет зашифрований.

1.2 Проблема розподілу часток секрету

Однією з проблем розподілу часток секрету є те, що вони часто можуть бути втрачені або скомпрометовані. Акціонери можуть померти, втратити свої частки або їх можуть вкрасти. А в разі втрати хоча б одного з членів групи, секрет буде загублений для всієї групи безповоротно. Інколи акціонери самі стають шахраями. Коли розподіляється багато різних часток, також непрактично і неефективно вимагати від усіх акціонерів відновити секрет.

1.3 Порогова схема як вирішення проблеми

Порогова схема (*threshold scheme*) пропонує вирішення проблеми розподілу часток секрету.

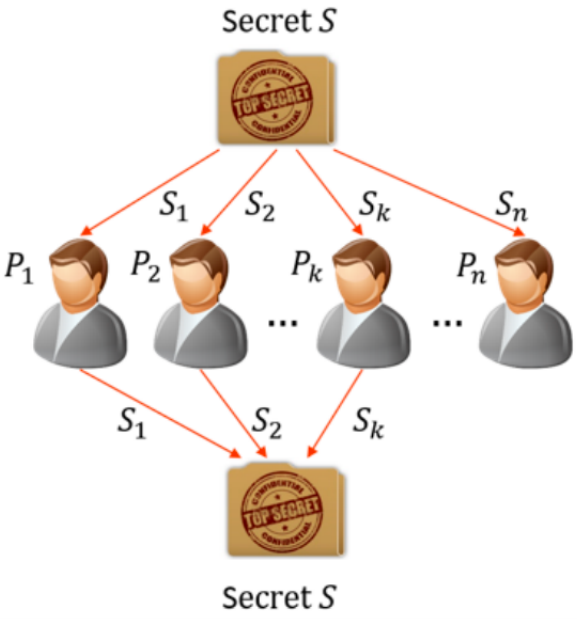

Рисунок 1.3 – Порогова схема розподілу секрету

Порогова схема — це метод розподілу секрету, який дозволяє відновити секрет, навіть якщо деякі з часток секрету втрачені або скомпрометовані. Це відбувається завдяки тому, що для відновлення початкового секрету вимагається лише частина частинок секрету, на які був розділений.

1.3.1 Найпростіша порогова схема

Ви можете взяти будь-яке повідомлення (секретний рецепт, коди запуску, ваш список білизни тощо) і розділити його на n частин, які називаються тіньовими потоками або спільними ресурсами, так що будь-які m із них можна використовувати для реконструкції повідомлення. Це називається (m,n)-порогова схема.

Приклад найпростішої порогової схеми:

За допомогою (3,4)-порогової схеми Трент може розділити свій секретний рецепт соусу між Алісою, Бобом, Керол і Дейвом, щоб будь-які троє з них могли об'єднати свої тіні та реконструювати повідомлення. Якщо Керол у відпустці, Аліса, Боб і Дейв можуть це зробити. Якщо Боба переїде автобус, Аліса, Керол і Дейв зможуть це зробити. Однак, якщо Боба переїде автобус, коли Керол у відпустці, Аліса та Дейв не зможуть відновити повідомлення самостійно.

1.3.2 Загальні порогові схеми

Загальні порогові схеми ще більш універсальні. Будь-який сценарій спільного використання, який ви можете собі уявити, можна змоделювати. Ви можете розділити повідомлення між людьми у вашій будівлі так, щоб для його реконструкції вам знадобилося сім людей з першого поверху та п'ять людей з другого поверху якщо не буде залучено когось із третього поверху. У такому випадку вам лише потрібна ця особа та троє людей з

першого поверху та двоє людей з другого поверху, за винятком випадків, коли хтось із четвертого поверху задіяний. У такому випадку вам потрібна ця особа та одна особа з третього поверху, або ця особа та двоє людей з перший поверх і одна особа з другого поверху і т.д. Цю ідею винайшли незалежно один від одного Аді Шамір і Джордж Блеклі, а також ретельно досліджував Гас Сіммонс в своїх алгоритмах.

Висновки до розділу 1

В цьому розділі ми розглянули важливу криптографічну задачу, яка дозволяє безпечно ділитися секретом між групою учасників – розділення секрету. Також розглянули існуючі різні схеми розділення секрету, які мають різні характеристики та ступінь стійкості до атак; проблему розподілу часток секрету та її вирішення – порогові схеми. В результаті було визначено, що розділення секрету є важливим інструментом для забезпечення безпеки та конфіденційності інформації. А порогові схеми – це один із найефективніших способів розподілу секрету між групою учасників.

2 СПОСОБИ РОЗДІЛЕННЯ СЕКРЕТУ В БАЗОВИХ ПРОТОКОЛАХ

2.1 Розділення секрету без Трента

Банк хоче, щоб його сховище відкрилося, лише якщо троє з п'яти співробітників введуть свої ключі. Це звучить як базова (3,5)-порогова схема, але є підступ. Ніхто не повинен знати весь секрет. Немає Трента, щоб розділити секрет на п'ять частин. Існують протоколи, за якими п'ятеро офіцерів можуть створити секрет і кожен отримає шматочок, так що жоден з офіцерів не дізнається секрету, доки всі не відновлять його [3].

2.2 Розширені порогові схеми розділення секрету

Попередні приклади ілюструють лише найпростіші порогові схеми. Далі буде використано алгоритм Шаміра, хоча будь-який з інших буде працювати.

Щоб створити схему, у якій одна людина важливіша за іншу, дайте цій людині більше тіней. Якщо для відтворення секрету потрібно п'ять тіней і одна людина має три тіні, а всі інші мають лише одну, тоді ця особа та ще двоє людей можуть відтворити секрет. Без цієї людини знадобиться п'ять, щоб відтворити секрет. Двоє або більше людей можуть отримати кілька тіней. У кожної людини може бути різна кількість тіней. Незалежно від того, як тіні розподілені, будь-яка m з них може бути використана для відновлення секрету. Хтось із $m-1$ тіней, будь то одна особа чи ціла кімната людей, не може цього зробити. Крім цього є варіанти, коли приймають участь дві ворожі делегації. Ви можете поділитися секретом, щоб відтворити секрет двом особам із 7 у делегації A та 3 особам із 12 у делегації B. Складіть поліном третього ступеня, який є добутком лінійного виразу на квадратичний вираз. Дайте кожному з делегації A тінь, яка є результатом оцінки лінійного рівняння; дайте кожному з делегації B тінь,

яка є оцінкою квадратного рівняння. Будь-які дві тіні від Делегації A можна використати для реконструкції лінійного рівняння, але незалежно від того, скільки інших тіней має група, вони не можуть отримати жодної інформації про секрет. Те саме стосується делегації B: вони можуть зібрати три тіні разом, щоб реконструювати квадратне рівняння, але вони не можуть отримати жодної

2.3 Розділення секрету з шахраями

Існує багато способів обдурити за допомогою порогової схеми. Оскільки при розподілі секрету гарантується, що якщо будь-який учасник отримає секрет, інші учасники також отримають. Таким чином в схемі можуть бути шахраї, приховані в учасниках, які можуть загрожувати компроментації секрету. Для боротьби з шахраями використовують спеціальну схему розділення секрету з шахраями. Розглянемо її далі [4].

Алгоритм "Розділення секрету з шахраями"модифікує стандартну (m, n)-порогову схему для виявлення шахраїв. Це буде продемонстровано за допомогою схеми Лагранжа, хоча вона також працює з іншими.

Виберіть просте число p, яке одночасно більше за n і більше за $\frac{(s-1)(m-1)}{e+m}$, де s – найбільший можливий секрет, а e – ймовірність успішного шахрайства. Ви можете зробити e настільки малим, скільки хочете; це лише ускладнює обчислення. Побудуйте свої тіні, як і раніше, за винятком використання замість 1, 2, 3, . . . , n для x_i; оберіть випадкові числа від 1 до $p-1$ для x_i.

Тепер, коли шахрай пробирається на таємну нараду з реконструкції зі своєю фальшивою часткою, велика ймовірність того, що його частка буде неможливою. Неможлива таємниця – це, звичайно, фальшива таємниця.

На жаль, хоча шахрая і викривають, він все одно дізнається секрет (припускаючи, що є m інших дійсних спільних ресурсів). Інший протокол, запобігає цьому. Основна ідея полягає в тому, щоб мати серію з k секретів, щоб жоден з учасників не знав заздалегідь, який правильний. Кожен секрет

більший за попередній, за винятком справжнього секрету. Учасники об'єднують свої тіні, щоб генерувати один секрет за іншим, поки не створять секрет, менший за попередній. Це правильний варіант.

Ця схема викриє шахраїв завчасно, до того, як буде згенеровано секрет. Також бувають ускладнення, коли учасники доставляють свої тіні по одному.

Висновки до розділу 2

В даному розділі було розглянуто різні способи розділення секрету в базових протоколах. А конкреніше – метод розділення секрету без Трента, який не потребує третьої сторони (Трента) для розподілу секрету; розширені порогові схеми розділення секрету, які дозволяють учасникам динамічно приєднуватися та виходити з групи, а також змінювати поріг відновлення секрету; схеми розділення секрету з шахраями, які стійкі до атак зловмисників, що можуть отримати доступ до частин секрету. Кожен з цих методів має свої переваги та недоліки. Вибір найкращого методу залежить від конкретних потреб та вимог до безпеки.

3 СПОСОБИ РОЗДІЛЕННЯ СЕКРЕТУ ЗА ДОПОМОГОЮ АСИМЕТРИЧНИХ АЛГОРИТМІВ

3.1 Розділення секрету RSA

Розділення секрету RSA — це метод розподілу секрету між групою учасників, який відбувається наступним чином:

1) Секрет шифрується за допомогою відкритого ключа RSA кожного учасника;

2) Зашифровані частини секрету передаються відповідним учасникам.

Відновлення ж секрету RSA відбувається наступним чином:

1) Кожен учасник розшифровує свою частину секрету за допомогою свого закритого ключа;

2) Розшифровані частини секрету потім об'єднуються для відновлення оригінального секрету.

Головними перевагами алгоритму RSA є безпека: секрет не може бути відновлений без приватних ключів учасників та гнучкість: поріг відновлення може бути встановлений таким чином, що для відновлення секрету необхідна певна кількість учасників.

Але при цьому алгоритм RSA є нестійким до атак зловмисників, які мають доступ до відкритих ключів учасників та нестійким до квантових атак.

3.2 Розділення секрету ECC

Розділення секрету ECC (Elliptic Curve Cryptography) — це метод розподілу секрету між групою учасників, який відбувається наступним чином:

1) Секрет перетворюється на точку на еліптичній кривій;

2) Ця точка потім розбивається на n частин, по одній для кожного

учасника;

3) Кожна частина потім шифрується за допомогою відкритого ключа ECC відповідного учасника;

4) Зашифровані частини секрету передаються відповідним учасникам.

Відновлення ж секрету ECC відбувається наступним чином:

1) Кожен учасник розшифровує свою частину секрету за допомогою свого закритого ключа;

2) Розшифровані частини секрету потім об'єднуються для відновлення оригінальної точки на еліптичній кривій;

3) Секрет після витягується з цієї точки.

Головними перевагами алгоритму ECC є безпека: якщо приватні ключі учасників є безпечними та стійкість до квантових атак.

Але при цьому алгоритм ECC – не стійкий до атак зловмисників, які мають доступ до відкритих ключів учасників і складніший у розумінні та реалізації за розділення секрету RSA.

3.3 Схема Shamir's Secret Sharing

Схема Shamir's Secret Sharing — це алгоритм, вперше запропонований у 1979 році відомим ізраїльським криптографом Аді Шаміром. Він дозволяє розбивати інформацію на багато частин, при цьому вимагаючи лише частину цих частин для відновлення початкового секрету.

Це означає, що замість того, щоб вимагати всіх частин для відновлення початкового секрету, схема Шаміра вимагає мінімальної кількості частин – цей мінімум називається *порогом*.

Розділення секрету Шаміра — це метод розподілу секрету між групою учасників, який відбувається наступним чином:

1) Секрет ділиться на n частин, де n – це кількість учасників;

2) Кожному учаснику надається поліноміальна частка ступеня $m-1$,

де m – це поріг відновлення.

Для того, щоб відновити секрет, необхідно досягти певного порогу. Якщо є щось менше, ніж поріг, секрет не може бути відновлений, таким чином роблячи розділення секрету за Шаміром захищеним від супротивника – зловмисника, який має необмежену обчислювальну потужність.

Однією з переваг алгоритму Шаміра є те, що він є гнучким і розширюваним – тобто власник секрету може додавати, змінювати або видаляти частки в будь-який час, якщо захоче, без зміни початкового секрету. А також він стійкий до атак зловмисників, які мають доступ до відкритих ключів учасників, і ще стійкий до квантових атак, оскільки ґрунтується на інтерполяції многочленів, яка є проблемою, яка, є складною для квантових комп'ютерів.

Але при цьому алгоритм Шаміра менш ефективний, ніж RSA або ECC, та крім цього – необхідно зберігати додаткову інформацію (наприклад, коефіцієнти полінома), щоб відновити секрет.

3.4 Порівняння ефективності алгоритмів за обраним критерієм

Для порівняння ефективності алгоритмів було взято в якості критерію – кількість обчислювальних операцій, необхідних для розподілу та відновлення секрету, де:

– n - кількість учасників

– m - поріг відновлення.

Алгоритм	**Розподіл**	**Відновлення**
RSA	$O(n^2)$	$O(m^2)$
ECC	$O(n^2)$	$O(n)$
Схема Шаміра	$O(n^3)$	$O(n^2)$

Також було проведено загальне порівняння алгоритмів:

Характеристика	RSA	ECC	Схема Шаміра
Безпека	Безпечний, якщо приватні ключі учасників є безпечними	Безпечний, якщо приватні ключі учасників є безпечними	Стійкий до атак зловмисників, які мають доступ до відкритих ключів учасників
Стійкість до квантових атак	Не стійкий	Стійкий	Стійкий
Ефективність	Ефективний	Ефективний	Менш ефективний
Складність	Простіше зрозуміти та реалізувати	Може бути складніше зрозуміти та реалізувати	Може бути складніше зрозуміти та реалізувати

Рисунок 3.1 – Загальне порівняння

Висновки до розділу 3

В даному розділі було розглянуто та порівняно різні способи розділення секрету за допомогою асиметричних алгоритмів. Також визначено, що розділення секрету не може гарантувати абсолютну безпеку секрету, але може значно ускладнити його розкриття зловмисниками. Використання методів розділення секрету може значно підвищити безпеку та конфіденційність інформації.

В результаті порівняння маємо наступне:

• RSA має найгіршу ефективність при відновленні секрету, але вона проста у реалізації + використовує експоненційні операції, які є обчислювально складними;

• ECC має кращу ефективність при відновленні секрету, але вона складніша у реалізації + використовує експоненційні операції, які є обчислювально складними;

• Схема Шаміра має найгіршу ефективність при розподілі секрету, але вона стійка до атак зловмисників, які мають доступ до відкритих ключів учасників + використовує інтерполяцію многочленів, яка є менш обчислювально складною.

ВИСНОВКИ

У ході дослідження було проведено порівняльний аналіз реалізацій розділення секрету за допомогою різних асиметричних алгоритмів. А також було проведено порівняння ефективності цих алгоритмів за обраним критерієм.

В результаті визначено, що:

– RSA може бути хорошим вибором, якщо важлива гнучкість та ефективність.

– ECC може бути хорошим вибором, якщо важлива стійкість до квантових атак.

– Схема Шаміра може бути хорошим вибором, якщо важлива стійкість до атак зловмисників, які мають доступ до відкритих ключів учасників.

Таким чином, найкращий метод розділення секрету для конкретного застосування залежатиме від конкретних вимог безпеки та продуктивності.

ЛІТЕРАТУРА

1. Keyless. *Shamir's Secret Sharing: A beginner's guide — keyless.io* https://keyless.io/blog/post/a-beginners-guide-to-shamir-s-secret-sharing. Бер. 2020.
2. Вікіпедія. *Розділення секрету* 2023. https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B4%D1%96%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D1%81%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D1%83.
3. Bruce, S. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)* 20-е вид. (John Wiley & Sons, Inc., 2015).
4. Tompa, M. & Woll, H. *How to share a secret with cheaters.* 1989. https://doi.org/10.1007/BF02252871.