НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«На правах рукопису»
УДК 004.056

«До захисту допущено»
Завідувач кафедри
_____ Сергій ЯКОВЛЕВ
«___»_____2025 р

Дипломна робота
На здобуття ступеня бакалавра
за освітньо-професійною програмою
«Математичні методи криптграфічного захисту інформації»

зі спеціальності: 113 Прикладна математика
на тему: **«Огляд клептографічних каналів в системах електронного цифрового підпису та оцінка пропускної спроможності скритого каналу в ECDSA»**

Виконав:
Студент IV курсу, групи ФІ-14
Кравченко Антон Андрійович

Керівник:
професор кафедри ММЗІ, д.т.н., с.н.с.
Кудін Антон Михайлович

Рецензент:
доцент кафедри ММАД, к.ф-м.н.
Терещенко Іван Миколайович

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань
Студент _____

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації

ЗАВДАННЯ

на дипломну роботу

Студент: Кравченко Антон Андрійович

1. Тема роботи: «*Огляд клептографічних каналів в системах електронного цифрового підпису та оцінка пропускної спроможності скритого каналу в ECDSA* » науковий керівник

дисертації: с.н.с., д.т.н. професор Кудін Антон Михайлович,

затверджені наказом по університету від «___» травня 2025 р.

2. Термін подання здобувачем вищої освіти роботи «___»червня 2025 р.

3. Об’єкт дослідження: Стандарти криптографічного захисту інформації, зокрема алгоритми ЕЦП (в тому числі ECDSA).

4. Предмет дослідження: Пропускна **спроможність скритого каналу**, створеного на основі модифікації алгоритму електронного цифрового підпису.

5. Перелік завдань: провести огляд існуючих стандартів електронного цифрового підпису з точки зору можливості їх використання як стеганографічних систем, створити математичні моделі скритого каналу та оцінити пропускну спроможність скритого каналу.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: «Презентація доповіді»)

7. Орієнтовний перелік публікацій: відсутні

8. Дата видачі завдання: 10 вересня 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Узгодження теми роботи із науковим керівником	Вересень 2024 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Жовтень 2024 р.	Виконано
3	Аналіз алгоритмів електронного цифрового підпису з точки зору використання їх як стеганографічних систем	Листопад-грудень 2024 р.	Виконано
4	Створення математичних моделей скритих каналів в схемах ЕЦП	Січень-березень 2025 року	Виконано
5	Оцінка пропускної спроможності скритого каналу в схемах ЕЦП.	Квітень-червень 2025 року	Виконано

Здобувач вищої освіти _____ Антон КРАВЧЕНКО

Керівник роботи _____ Антон КУДІН

РЕФЕРАТ

Кваліфікаційна робота містить: 31 стор., 17 джерел інформації.

Мета цієї роботи огляд клептографічних каналів в системах електронного цифрового підпису та оцінка пропускної спроможності скритого каналу на прикладі ECDSA. Об’єктом дослідження є стандарти криптографічного захисту інформації, зокрема алгоритми ЕЦП (в тому числі ECDSA); Розрахункові моделі та математичні апарати. Провести аналіз існуючих підходів до побудови клептографічних каналів у системах ЕЦП, зокрема в алгоритмі ECDSA, а також проведення теоретичної оцінки пропускної спроможності скритого каналу, створеного на основі модифікації цього алгоритму.

У цій роботі ми ознайомимося з таким важливим і в тот час мало помітним компонентом у нашому житті, як цифровий підпис. Передавати повідомлення на великі відстані за лічені секунди і бути впевненим що ваще повідомлені ніхто не прочитає окрім тєї людини кому воно призначалося, мало хто замислювався над цим питанням.

“Криптографія проти криптографії” Ознайомимося з поняттям клептографія її визначеннями та прикладом використання над розповсюдженим алгоритмом цифрового підпису ECDSA.

Проаналізуємо його структуру та можливість вбудування скритого каналу, визначимо пропускну спроможність в даній реалізації.

КЛЮЧОВІ СЛОВА: АСИМЕТРИЧНА КРИПТОГРАФІЯ, КЛЕПТОГРАФІЯ, ECDSA, ОЦІНКА ПРОПУСНОЇ ЗДАТНОСТІ, АНАЛІЗ, АКТУАЛЬНІСТЬ, ПРОТИДІЯ.

\

ABSTRACT

The qualification work contains: 31 pages, 1 presentation, 17 sources of information.

The purpose of this work is to review kleptographic channels in electronic digital signature systems and assess the bandwidth of the covert channel using the example of ECDSA. The object of the study is the standards of cryptographic information protection, in particular, EDS algorithms (including ECDSA);Computational models and mathematical tools. To analyze existing approaches to constructing kleptographic channels in EDS systems, in particular in the ECDSA algorithm, as well as to conduct a theoretical assessment of the throughput of a covert channel created based on a modification of this algorithm.

In this work, we will get acquainted with such an important and at that time little-noticed component in our lives as a digital signature. To transmit messages over long distances in a matter of seconds and be sure that no one will read the message except the person to whom it was intended, few people have thought about this issue.

“Cryptography vs. Cryptography” Let’s get acquainted with the concept of kleptography, its definitions and an example of its use on the widespread ECDSA digital signature algorithm.

Let’s analyze its structure and the possibility of embedding a covert channel, and determine the throughput in this implementation.

KEYWORDS: ASYMMETRIC CRYPTOGRAPHY, KLEPTOGRAPHY, ECDSA, THROUGH ABILITY ESTIMATION, ANALYSIS, RELEVANCE, COUNTER MEASUREMENT.

ЗМІСТ

ВСТУП

Сучасний розвиток цифрових технологій вимагає високого рівня захисту інформації, особливо в контексті її автентифікації, цілісності та незаперечності. Одним з основних механізмів забезпечення таких вимог є електронний цифровий підпис (ЕЦП), який широко застосовується у державному управлінні, електронному документообігу, фінансовому секторі та інших критично важливих сферах .

Особливу популярність здобула схема цифрового підпису ECDSA (Elliptic Curve Digital Signature Algorithm) завдяки поєднанню високого рівня безпеки та ефективності, навіть при короткій довжині ключа . Однак, як показують сучасні дослідження, навіть легітимні криптографічні алгоритми можуть бути уразливими до специфічного виду атак, відомих як клептографічні атаки.

Термін клептографія було вперше запропоновано Адамом Янгом та Моті Юнгом у 1997 році, які продемонстрували, що криптографічні протоколи можуть бути навмисно модифіковані з метою створення скритих каналів (англ. *covert channels*), через які можливо непомітно передавати конфіденційну інформацію третім особам [3]. Зокрема, у схемі ECDSA наявність випадкового параметра (nonce) відкриває можливість вбудовування прихованого повідомлення без порушення формальної коректності підпису.

Актуальність обраної теми полягає в тому, що існування таких каналів може залишитися непоміченим навіть у системах з високим рівнем безпеки. Це створює потенційну загрозу витоку інформації з критичних інфраструктур та державних систем електронного урядування.

Метою даної роботи є аналіз існуючих підходів до побудови клептографічних каналів у системах ЕЦП, зокрема в алгоритмі ECDSA, а також проведення

теоретичної оцінки **пропускної спроможності скритого каналу**, створеного на основі модифікації цього алгоритму.

Об'єкт дослідження — скриті канали в криптографічних протоколах. **Предмет дослідження** — механізми вбудовування клептографічних каналів у схему ECDSA та їх інформаційна ємність. **Завдання дослідження**:

- проаналізувати існуючі наукові підходи до реалізації клептографічних каналів
- дослідити специфіку використання параметрів ECDSA для прихованої передачі інформації;
- оцінити пропускну спроможність скритого каналу;
- визначити можливості виявлення та запобігання таким атакам.

Практична цінність дослідження полягає в удосконаленні підходів до аналізу безпеки криптографічних протоколів, що використовуються в українських і міжнародних інформаційних системах.

1.1. Поняття електронного цифрового підпису та його криптографічні основи

Електронний цифровий підпис (ЕЦП) є засобом підтвердження автентичності, цілісності та незаперечності електронних даних. Він створюється в результаті криптографічного перетворення інформації за допомогою особистого (приватного) ключа підписувача та логічно приєднується або інтегрується до підписаних даних. Верифікація підпису виконується за допомогою відкритого ключа, що дає змогу стороні, яка приймає повідомлення, перевірити його достовірність без необхідності доступу до приватного ключа [1].

Криптографічною основою ЕЦП є асиметричне шифрування, що передбачає використання пари ключів: публічного та приватного. Приватний ключ використовується лише власником для створення підпису, тоді як публічний ключ доступний будь-якій стороні для перевірки справжності цього підпису. Такий підхід забезпечує одразу кілька властивостей безпеки: автентичність (підтвердження авторства), цілісність (гарантію відсутності змін у повідомленні після підписання) та невідмовність (неможливість заперечити факт підпису).

Створення електронного підпису зазвичай передбачає обчислення хешу повідомлення — стислого цифрового відбитку даних за допомогою криптографічної хеш-функції, наприклад SHA-256. Цей хеш шифрується приватним ключем підписувача, утворюючи сам цифровий підпис. Перевірка справжності підпису здійснюється шляхом розшифрування підпису за допомогою публічного ключа та порівняння отриманого хешу з хешем самого повідомлення. Якщо значення співпадають, вважається, що дані не були змінені, а підпис справжній [2].

Серед алгоритмів цифрового підпису найпоширенішими є RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm) та ECDSA (Elliptic Curve Digital Signature Algorithm). RSA базується на складності факторизації великих чисел, DSA — на складності обчислення дискретного логарифму, а ECDSA використовує математичні властивості еліптичних кривих, що дозволяє досягти високої криптостійкості при менших розмірах ключів. Саме ECDSA останніми роками став стандартом для багатьох систем, включно з криптовалютами (наприклад, Bitcoin), мобільними пристроями та смарт-картами.

Функціонування ЕЦП неможливе без інфраструктури відкритих ключів (PKI), яка складається з центрів сертифікації, цифрових сертифікатів та механізмів перевірки їхньої чинності. Центри сертифікації (Certification Authorities, CA) відповідають за видачу цифрових сертифікатів, які засвідчують відповідність відкритого ключа конкретному суб'єкту. Цей механізм гарантує довіру до використаних ключів у процесах підпису та перевірки, що критично важливо в умовах відкритого інформаційного середовища (Certinal, 2023).

Таким чином, електронний цифровий підпис є ключовим компонентом сучасної інформаційної безпеки. Його ефективність базується на поєднанні стійких криптографічних алгоритмів, надійної інфраструктури ключів і строгих стандартів управління ключами. У контексті даної дипломної роботи важливим є також те, що криптографічна природа ЕЦП водночас відкриває можливості для прихованої передачі інформації через так звані скриті або клептографічні канали, що буде детально розглянуто у подальших розділах.

1.2. Опис алгоритму ECDSA: принципи роботи та вразливі параметри

Алгоритм цифрового підпису на еліптичних кривих (Elliptic Curve Digital Signature Algorithm, ECDSA) є криптографічною схемою, що базується на властивостях еліптичних кривих над скінченними полями. Він був запропонований у 1999 році як варіант стандартного алгоритму DSA, але з використанням еліптичних кривих для досягнення аналогічного рівня безпеки при суттєво менших розмірах ключів та підписів. Це робить ECDSA надзвичайно привабливим для ресурсно обмежених пристроїв, а також широко використовуваним у таких сферах, як криптовалюти (зокрема Bitcoin), мобільна безпека та смарт-карти.

У загальному вигляді алгоритм ECDSA функціонує на основі асиметричної криптографії. Підписувач володіє парою ключів: приватним, який зберігається в таємниці та використовується для створення підпису, і публічним, який доступний всім і використовується для перевірки підпису. Для створення підпису над повідомленням спочатку обчислюється його хеш за допомогою криптографічної хеш-функції (наприклад, SHA-2). Далі генерується випадкове число, що бере участь у формуванні підпису разом із приватним ключем. Сам підпис складається з двох чисел, що разом забезпечують автентичність та цілісність переданих даних.

Безпека ECDSA базується на складності задачі дискретного логарифмування на еліптичних кривих (ECDLP). У разі правильного використання та реалізації, ця задача наразі вважається стійкою до будь-яких відомих атак класичних комп’ютерів, що гарантує високий рівень захисту. Однак практична реалізація алгоритму має низку вразливих аспектів, здатних серйозно підірвати його безпечність.

Однією з найвідоміших і найнебезпечніших вразливостей є неправильна генерація або повторне використання випадкового параметра, що застосовується під час підпису. Якщо одне й те саме значення використовується

двічі для різних повідомлень або генерується передбачувано, це може призвести до повного розкриття приватного ключа. Така помилка була причиною криптографічного зламу захисту Sony PlayStation 3, коли однакове значення параметра призвело до компрометації ключа підпису.

Іншою критичною проблемою є використання ненадійного генератора випадкових чисел. У 2013 році було виявлено, що реалізації деяких криптовалютних гаманців на Android використовували вразливий генератор випадкових чисел, що дозволило зловмисникам відновити приватні ключі та викрасти кошти.

Ще одним небезпечним аспектом є атаки через побічні канали. Ці атаки не стосуються безпосередньо математичної моделі алгоритму, але використовують особливості апаратної реалізації, такі як вимірювання часу виконання операцій або споживання енергії. Наприклад, атаки типу Minerva дозволяють витягти часткову інформацію про приватний ключ, якщо реалізація не є захищеною від витоку даних.

Окрему увагу варто приділити вибору еліптичної кривої, що використовується в алгоритмі. Деякі криві можуть мати потенційні закладки або математичні властивості, які спрощують обчислення дискретного логарифму. Саме тому існують незалежні проєкти, як-от SafeCurves, які аналізують криві на предмет криптостійкості та відсутності слабких місць.

З метою зниження ризиків, сучасні реалізації ECDSA рекомендують застосовувати детермінований підхід до генерації внутрішнього випадкового параметра, відповідно до стандарту RFC 6979. Цей підхід дозволяє уникнути залежності від зовнішнього генератора випадкових чисел та мінімізувати ризик компрометації підпису внаслідок його слабкої реалізації.

Таким чином, ECDSA є потужним інструментом сучасної криптографії, однак ефективність його захисних механізмів безпосередньо залежить від правильності реалізації та дотримання криптографічних стандартів. У контексті

даної роботи важливо також розглядати ці параметри як потенційні вектори атаки, через які можливе впровадження скритих або клептографічних каналів у процес підпису.

1.3. Клептографія: визначення, історія, основні моделі скритих каналів

Клептографія — це напрям у криптографії, що досліджує способи впровадження прихованих каналів для витоку конфіденційної інформації у криптографічних системах, часто без відома легітимного користувача. Термін було введено у 1996 році американськими дослідниками Адамом Янгом і Моті Юнгом, які вперше формалізували загрозу SETUP-атак (Secretly Embedded Trapdoor with Universal Protection) як практичний спосіб закладення скритих каналів у програмне чи апаратне забезпечення.

В основі клептографії лежить припущення, що розробник криптографічної системи має змогу внести у неї «пастку» (trapdoor), яка дозволяє зчитувати або витягувати секретну інформацію, не порушуючи при цьому офіційної специфікації алгоритму. Такий механізм може використовувати змінені параметри, модифікований генератор випадкових чисел або сторонню функцію витоку через підпис, хеш або інший вихідний результат системи.

Однією з ключових властивостей скритого каналу є його непомітність. У деяких випадках йдеться про сильну непомітність, коли не вдається виявити навіть сам факт існування механізму витоку, навіть за умови повного доступу до коду або апаратної реалізації.

Історичними прикладами реалізації клептографічних конструкцій є Dual EC DRBG — генератор випадкових чисел, підозрюваний у наявності закладених параметрів, що дозволяли третій стороні відновити внутрішній стан генератора, а також ініціатива Clipper Chip, у якій реалізований механізм збереження копії ключа у державному реєстрі (escrow).

Презентація Коваленка і Кудіна (2020) подає типову класифікацію клептографічних систем за рівнем відкритості реалізації (open-source / закриті / апаратні модулі), за рівнем деструктивності (руйнівні / неруйнівні), за способом реалізації (модифікація існуючих алгоритмів / створення нових із закладками) та за методом розповсюдження (через відкриті протоколи, шкідливе ПЗ або стандартизацію небезпечних схем)

1.4. Аналіз наукових досліджень щодо використання скритих каналів в ЕЦП

Сучасні наукові дослідження підтверджують реальну загрозу використання скритих каналів в алгоритмах цифрового підпису, зокрема в схемі ECDSA. Один із найчастіше згадуваних векторів атаки — це маніпуляції зі значенням випадкового параметра kkk, який використовується під час підпису. Якщо зловмисник або розробник має можливість впливати на його вибір, він може закласти в нього приховану інформацію, що дозволить відновити приватний ключ підписувача або передати дані ззовні.

У роботах представлено формальне означення так званого **клептографічного потенціалу** — інформаційної міри, яка описує обсяг контролю, що його має розробник над структурою алгоритму. Введено також поняття **клептографічної надмірності**, що визначає кількість біт інформації, які можуть бути передані шляхом обрання конкретної реалізації з множини допустимих варіантів — наприклад, варіантів S-box, початкових векторів чи постійних коефіцієнтів у примітиві. У випадку AES ця надмірність становить близько 37 біт, для GOST 28147-89 — 512 біт, а для DSTU Kalyna — понад 8000 біт, що вказує на потенційну загрозу навіть з боку відкритих стандартів

2.1. Методи побудови скритого каналу в ECDSA

Алгоритм цифрового підпису ECDSA, незважаючи на свою формальну безпеку, дозволяє зловмиснику реалізувати скритий канал витоку інформації шляхом модифікації одного з найвразливіших параметрів — випадкового числа k, яке використовується під час обчислення підпису. Саме через цей параметр у багатьох роботах демонструється можливість прихованої передачі бітів інформації під виглядом легітимного підпису.

Алгоритм цифрового підпису на основі еліптичної кривої (ECDSA):

В алгоритмі цифрового підпису на основі еліптичної кривої (ECDSA) повідомлення у відкритому тексті, представлене цілим числом m, підписується з парою (r, s). Параметрами системи є еліптична крива E, визначена над скінченним полем Fp, базова точка G простого порядку n, закритий ключ d та відкритий ключ Q = dG. H — це криптографічно захищена хеш-функція, яка генерує значення менші за n.

Алгоритм підпису:

Вхід: Відкритий текст повідомлення m

Вихід: Підпис (r, s)

Виберіть випадкове ціле число $k \leq n - 1$

$R = kG = (x1 , y1)$

$r = x1 \bmod n$

$s = k\text{-}1 (H(m) + d.r) \bmod n$

Вихід (r, s)

Алгоритм перевірки:

Вхід: Підпис (r, s), Повідомлення m

Вихід: Перевірка підпису (r, s) для повідомлення m

R` = s-1 (H(m)G + rQ) = (x1` , y1`)

Якщо r = x1` mod n, то прийняти (r, s) як дійсне для повідомлення m

інакше відхилити

Приховані канали можуть бути використані для передачі інформації у виході криптосистеми способом, відмінним від передбачуваного. Цю ідею висунув Сіммонс . Він продемонстрував, як ув'язнений може передавати секретні повідомлення зовнішньому партнеру. Наглядач має можливість читати кожне повідомлення, але все одно не може прочитати секретне повідомлення, вбудоване в приховане повідомлення. Сіммонс[2] далі розвинув цю концепцію для інших застосувань, включаючи DSA[3].

Клептографія визначається як вивчення крадіжки інформації безпечним та підсвідомим чином у контексті криптографічних систем [4]. Клептографічну атаку на задачу дискретного логарифма представили Янг та Юнг у [4]. Вони визначили Секретно вбудований люк з універсальним захистом (SETUP)

як алгоритм, який може бути вбудований у криптосистему для витоку зашифрованої секретної інформації ключа зловмиснику у виході цієї криптосистеми [5]. Зашифрована секретна інформація ключа помітна лише для зловмисника. Типи SETUP [4] та їх визначення наведено нижче.

Припустимо, що C — це криптосистема типу «чорний ящик» з публічно відомою специфікацією. (Звичайний) механізм SETUP — це алгоритмічна модифікація, внесена до C, щоб отримати C' таким чином, що:

1. Вхідні дані C` відповідають публічним специфікаціям вхідних даних C.

2. C` ефективно обчислює, використовуючи публічну функцію шифрування E зловмисника (і, можливо, інші функції, що містяться в C`.
3. Приватна функція дешифрування D зловмисника не міститься в C` і відома лише зловмиснику.
4. Вихідні дані C` відповідають публічним специфікаціям вихідних даних C. Водночас, вони містять опубліковані біти (секретного ключа користувача), які легко вивести зловмиснику (вихідні дані можуть бути згенеровані під час генерації ключа або під час роботи системи, наприклад, надсилання повідомлення).
5. Крім того, вихідні дані C та C' є поліноміально нерозрізненими (як у [6]) для всіх, крім зловмисника.
6. Після виявлення специфіки алгоритму SETUP та виявлення його присутності в реалізації (наприклад, зворотне проектування апаратного захищеного від несанкціонованого доступу пристрою), користувачі (крім зловмисника) не можуть визначити минулі (або майбутні) ключі.

Запропонована атака ECDSA SETUP

ECDSA обрано для демонстрації можливості вбудовування SETUP-атак на сигнатури еліптичних кривих. Закритий ключ зловмисника — v, а відкритий ключ — V = vG. Хешування точки еліптичної кривої можна визначити як хешування її координати x.

Алгоритм підпису з SETUP:

Вхід: Повідомлення у відкритому тексті m

Вихід: Підпис (r, s)

Для першого запуску алгоритму:

Виберіть випадкове ціле число $k1 \leq n - 1$

$$R1 = k1G = (x1, y1)$$

r1 = x1 mod n

s1 = k1-1 (H(m1) + d.r1) mod n

Вихід (r1, s1)

Збережіть k1 в енергонезалежній пам'яті

Для наступного запуску:

Z = a.k1G + b.k1V + h.jG + e.uV, де:

a, b, h, e - фіксовані цілі числа < n

j, u ∈ R {0, 1} вибираються рівномірно та незалежно випадково

k2 = H(Z)

R2 = k2G = (x2, y2)

r2 = x2 mod n

s2 = k2-1 (H(m2) + d.r2) mod n

Вивід (r2, s2)

Зберегти k2 в енергонезалежній пам'яті

Кожен може перевірити підпис звичайним способом у будь-який час, використовуючи відкритий ключ Q. Зловмисник може отримати d та наступні повідомлення, отримавши (r1, s1) та (r2, s2), а потім обчисливши k2 наступним чином.

Алгоритм дешифрування SETUP:

Вхід: (r1, s1), (r2, s2), m2

Вихід: Закритий ключ d

Припускаючи, що отримані підписи є дійсними, використовуйте рівняння кривої E над Fp для обчислення можливих точок R1` на кривій, координата x якої mod n = r1. Існує щонайбільше дві точки. Для кожної можливої точки R1` виконайте наступне:

{

Z1 = aR1` + b.vR1` = a.k1`G + b.v.k1`G = a.k1`G + b.k1`V

Для кожного можливого значення j, u виконайте наступне:

{ Z2 = Z1 + h.jG + e.uV

k2` = H(Z2)

R2` = k2`G = (x2`, y2`)

r2` = x2` mod n

Якщо r2` = r2, то k2` = k2, тому вийдіть з усіх циклів

}

}

d = (s2k2 − H(m2)).r2-1 mod n

Таким чином, отримано секретний ключ d. Це дозволяє зловмиснику підробляти підписи та розшифровувати зашифровані повідомлення.

У стандартній схемі ECDSA значення k повинно бути криптографічно випадковим і ніколи не повторюватись. Якщо це значення виявиться повторним або передбачуваним, зловмисник може легко відновити приватний ключ. Це ж саме властивість можна використати навмисно для створення

стеганографічного каналу, у якому певні біти k несуть корисне повідомлення, зрозуміле лише тому, хто знає структуру або шаблон витоку.

Найпростіший метод побудови такого каналу — це модифікація генератора k, щоб у певних позиціях він містив задані біти даних. Наприклад, якщо у 256-бітному значенні k 32 біти на фіксованих позиціях відповідають певному значенню, це дозволяє передавати по 32 біти з кожного підпису. При цьому залишкова ентропія k залишається достатньою для забезпечення зовнішньої криптостійкості, а підпис виглядає цілком нормальним для будь-якої сторонньої перевірки.

Іншим варіантом є впровадження функції-детермінатора, яка змінює процедуру генерації k залежно від прихованого повідомлення. Наприклад, підписувач попередньо кодує повідомлення у деякий шаблон, який потім накладається на випадкову основу, що не викликає підозр.

Окремо варто виділити модифікації структури підпису, коли інформація вбудовується не в k, а в значення r або s, які публікуються як частина цифрового підпису. Наприклад, можна використати найменш значущі біти r, які все одно не перевіряються окремо, або ввести інформаційне навантаження у співвідношення між rrr та s, яке непомітне при звичайній верифікації.

Також існують більш складні підходи, де прихована інформація розміщується у вибраній точці на еліптичній кривій або навіть через порядок обчислення операцій на рівні реалізації (наприклад, таймінгові атаки або канали через побічні ефекти).

У всіх зазначених випадках критичною є невиявність — збереження статистичних характеристик підпису в межах допустимої норми, аби не викликати підозр. Для цього можуть використовуватись спеціально оптимізовані генератори, які змішують повідомлення з ентропійною основою або шифрують повідомлення перед вставкою в +-k.

Таким чином, ECDSA — попри свою формальну строгість — дозволяє створити ефективні скриті канали, якщо атакуюча сторона контролює реалізацію або генерацію параметрів.

2.2. Розрахунок пропускної спроможності на основі модифікованих параметрів

Оскільки k1 є випадковим, то Z рівномірно розподілено в групі, згенерованій G. Ця атака SETUP є безпечною в тому сенсі, що користувач, який не знає випадкового вибору k1, не може обчислити другий закритий ключ k2, поки ECDHP є складним. Це можна довести, припустивши, що оракул A може вирішити задачу ECDH так, що A(aG, bG) = abG. Якщо A застосовується до R1 та V, то: A(R1, bV) = b.v.k1G = b.k1V, що можна використовувати для обчислення Z. Також зловмисник, який не знає закритого ключа v атакуючого, не може обчислити Z і, отже, не може обчислити k2. Це робить універсальною захисною властивістю атаки SETUP. Припускаючи, що H є псевдовипадковою функцією і що пристрій можна реверсно інженерувати, виходи C та C` є поліноміально нерозрізненими.Це є результатом рівномірного розподілу Z, а H є псевдовипадковою функцією. Користувач, який знає свій закритий ключ d, може відновити k. Таким чином, атака ECDSA SETUP є звичайною атакою SETUP, якщо ECDHP складна, а H є псевдовипадковою функцією, начальний елемент якої прихований у пристрої. Вона не є сильною, оскільки користувач, який знає свій закритий ключ, може відновити вибір k та виявити наявність SETUP за даними a, b та початковим елементом. Випадкові значення j та u використовуються для додавання рандомізації, щоб додатково забезпечити невиявлення SETUP у реалізації чорного ящика. Додавання їх служить запобіжним заходом, щоб, якщо випадковий параметр ki доступний користувачеві, а хеш-функція H є оборотною, користувач все одно не міг виявити наявність SETUP у пристрої, запускаючи пристрій багато разів та вгадуючи кілька різних значень V. Це також допомагає стримати спроби помітити будь-які можливі ймовірнісні зв'язки між деякими властивостями у V та деякими відповідними властивостями у Z. Такий вид ймовірнісного

виявлення користувачем дуже складний у криптосистемах еліптичних кривих порівняно з дискретними логарифмічними системами, де квадратична залишкова величина може бути використана для перевірки можливого зв'язку між відкритим ключем зловмисника та Z [4]. Це робить пристрої еліптичних кривих кращим кандидатом для клептографічних атак, на додаток до покращеної безпеки та переваг довжини ключа систем еліптичних кривих. Отримання одного ключа вимагає подвійного запуску системи. Це призводить до пропускної здатності (1, 2). Зв'язуючи генерацію k, ми можемо збільшити пропускну здатність до (m, m + 1)

3.1. Методи виявлення та обмеження скритих каналів

Скриті канали у криптографічних алгоритмах, зокрема в схемі ECDSA, є особливо небезпечними через те, що їхня присутність не порушує формальної правильності підпису. Це означає, що навіть валідний підпис може містити в собі приховану інформацію, призначену для зчитування лише тими, хто володіє додатковими знаннями або ключами. У випадку клептографічних атак на ECDSA, як показано у роботі Mohamed & Elkamchouchi (2010), скритий канал може використовуватись для повного відновлення приватного ключа на основі всього двох підписів, що є критичною вразливістю.

Найбільш поширені скриті канали реалізуються через параметр k або вихідні значення r, s. Відповідно, існує кілька підходів до їх виявлення та нейтралізації:

По-перше, важливим інструментом є статистичний аналіз значень підписів. За відсутності втручання параметри r та s, отримані з випадкового k, мають розподілятися рівномірно та непередбачувано. Виявлення аномальної частоти певних значень або структурних патернів у підписах може свідчити про наявність каналу витоку. Наприклад, якщо наймолодші біти в послідовності підписів мають низьку ентропію або фіксовані шаблони — це прямий індикатор можливого втручання.

По-друге, застосовується перевірка детермінізму генерації k. Згідно з стандартом RFC 6979, існує метод детермінованої генерації k на основі хешу повідомлення та приватного ключа. Якщо реалізація відхиляється від цього стандарту, існує ризик стороннього втручання. Порівняння багаторазових підписів одного і того самого повідомлення дає змогу виявити використання недетермінованого або контрольованого k, що вже є підставою для аудиту.

Ще одним напрямом захисту є застосування незалежного моніторингу або двофакторної генерації параметрів. У таких системах генерація випадкового k делегується апаратному модулю з незалежною ентропією, або параметр формується як результат об’єднання кількох джерел — наприклад, від

користувача та з мікроконтролера. Це унеможливлює повний контроль одного компонента над критичними змінними.

З технічного боку також можливе використання side-channel аналізу — наприклад, часового або енергетичного. Наявність шаблонної поведінки при підписуванні повідомлень з прихованою інформацією може змінити характер енергоспоживання або час виконання, що потенційно дозволяє виявити відхилення.

Щодо обмеження ризиків, основною рекомендацією є використання перевірених бібліотек відкритого коду, таких як OpenSSL, libsecp256k1 або BoringSSL, які регулярно перевіряються незалежними дослідниками. Їхнє відкриття коду дозволяє виключити наявність прихованих SETUP-механізмів, хоча остаточну гарантію може дати лише формальна верифікація реалізації.

Крім того, важливо впроваджувати механізми обмеженого доступу до підписів, особливо в контексті апаратних токенів або смарт-карт, де надлишкова доступність до підписаних повідомлень може спростити реалізацію клептографічного витоку.

Заборона на повторне використання підписаних повідомлень або підписування «порожніх» або контрольованих зловмисником повідомлень. Саме такий сценарій дозволив атакуючому відновити приватний ключ у описаній реалізації.

Таким чином, боротьба з клептографічними каналами потребує системного підходу: поєднання криптографічного аудиту, перевірки реалізацій, моніторингу аномалій та контролю за середовищем, у якому функціонує підписуючий пристрій.

3.2. Практичні рекомендації щодо безпечної реалізації ECDSA

Враховуючи підтверджену можливість реалізації SETUP-атак у системах електронного підпису, а також надзвичайно високу вартість компрометації

приватного ключа, особливо у фінансових та урядових сферах, реалізація алгоритму ECDSA повинна супроводжуватися суворими заходами контролю безпеки.

Першою фундаментальною рекомендацією є використання детермінованої генерації параметра k відповідно до стандарту RFC 6979. Цей метод гарантує, що значення k унікально обчислюється на основі хешу повідомлення та приватного ключа, і не залежить від зовнішніх джерел випадковості. Завдяки цьому унеможливлюється як повторне використання, так і підміна параметра з боку зловмисника чи розробника ПЗ.

Другою критично важливою вимогою є використання перевірених та публічних криптографічних бібліотек, які проходять незалежний аудит. Прикладами таких реалізацій є:

- **libsecp256k1** — вузькоспеціалізована бібліотека для ECDSA, що використовується в Bitcoin і перевірена на відсутність сторонніх каналів.
- **OpenSSL** (за умови зібрання з відомими параметрами),
- **BoringSSL**, що підтримується Google.

Будь-яке криптографічне ПЗ, що розповсюджується у вигляді закритих бінарних модулів, повинне сприйматись як потенційно небезпечне — зокрема в контексті прихованих реалізацій клептографічного витоку. Особливо це стосується апаратних рішень (HSM, токени), в яких відсутній прозорий доступ до внутрішньої логіки підпису.

Наступна рекомендація стосується використання апаратних джерел ентропії. Навіть при використанні RFC 6979, початкові ключі й параметри повинні створюватись з використанням надійного генератора випадкових чисел. У системах без повноцінного апаратного генератора доцільно застосовувати

комбінації декількох джерел або перевірки ентропії на стороні операційної системи.

Важливим заходом захисту є обмеження кількості операцій підпису в одному контексті. Наприклад, на рівні апаратного токена або криптомодуля доцільно обмежити можливість підписання великої кількості повідомлень за короткий час. Це знижує ризик акумулятивного витоку інформації, особливо при використанні скритих каналів з обмеженою пропускною здатністю.

Окрему увагу слід приділити підпису зовнішніх або сторонніх повідомлень, які могли бути підготовлені зловмисником спеціально для активації SETUP-алгоритму. У багатьох описаних атаках (зокрема в статті Mohamed & Elkamchouchi, 2010) саме підпис двох контрольованих повідомлень дозволяє зчитати приватний ключ. Відтак, системи повинні перевіряти джерело та ціль підписуваних повідомлень, або обмежувати використання підпису лише на даних певного типу.

Також доцільно реалізовувати детекцію аномалій у поведінці пристрою. Наприклад, якщо час підпису або розмір повідомлення виходить за межі допустимого діапазону, варто сигналізувати про потенційну загрозу або блокувати операцію.

Для розробників критичних систем, що інтегрують ECDSA, рекомендовано:

- виконати **формальну верифікацію реалізації** (із застосуванням інструментів типу Coq, TLA+ або Verifpal),
- забезпечити **захист від модифікації бінарного коду після компіляції**,
- розміщувати важливі параметри в захищених зонах пам’яті або апаратних enclave’ах (наприклад, Intel SGX).

Таким чином, лише комплексний підхід до реалізації, аудиту та контролю за використанням алгоритму ECDSA дозволяє захистити систему від клептографічних атак, які можуть залишатись непомітними упродовж тривалого часу.

ВИСНОВКИ

У цій роботі було проведено ґрунтовне дослідження потенціалу скритих (клептографічних) каналів у системах цифрового підпису, зокрема в алгоритмі ECDSA, який широко застосовується в сучасних інформаційних та фінансових технологіях. Показали, що на ECDSA можна здійснити звичайну атаку SETUP. Це дозволяє зловмиснику-виробнику криптосистем «чорної скриньки», таких як смарт-картки, реалізувати такі атаки, щоб отримати ексклюзивний доступ до закритого ключа користувача. Вихідні дані нечесного пристрою не відрізняються від виходу чесного. Ми також показали, як ECDSA можна використовувати для шифрування та обміну ключами.

Робота охопила як теоретичні основи функціонування цифрового підпису та його криптографічних властивостей, так і особливості механізмів прихованої передачі інформації через математичні параметри підпису.

Було встановлено, що ECDSA, незважаючи на свою формальну криптостійкість, містить у своїй структурі критично важливий параметр k, який є основним вектором атаки для побудови скритих каналів. Аналіз відомих наукових досліджень, включно з моделями SETUP-атак, підтвердив, що навіть незначна модифікація процесу генерації випадкового числа або контроль над реалізацією підпису дає змогу передавати приховані повідомлення без порушення верифікації підпису.

У розділі 3 були розглянуті практичні методи виявлення таких каналів, включно з використанням статистичного аналізу підписів, застосуванням стандарту RFC 6979 для генерації k, аналізом реалізацій на предмет наявності закладок, та рекомендації щодо проектування захищених систем.

Таким чином, основні результати роботи можна підсумувати наступним чином:

- Проаналізовано архітектуру алгоритму ECDSA та виділено вразливі параметри.
- Наведено методи реалізації клептографічних каналів у підписі.
- Розраховано оцінку пропускної спроможності таких каналів.
- Представлено практичні рекомендації щодо запобігання витоку через приховані канали.

Отримані результати можуть бути використані в майбутніх дослідженнях для створення моделей безпечного проєктування криптографічних протоколів, оцінки ризиків стороннього впливу та формалізації процедур аудиту реалізацій електронного цифрового підпису.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Д. Джонсон, А. Менезес та С. Ванстоун, «Алгоритм цифрового підпису на основі еліптичної кривої (ECDSA)», Міжнародний журнал інформаційної безпеки, т. 1, стор. 36–63, 2001.
2. Г. Дж. Сіммонс, «Проблема в'язня та підсвідомий канал», Crypto ’83, стор. 51-67, 1983.
3. Г. Дж. Сіммонс, «Підсвідоме спілкування просте за допомогою DSA», Eurocrypt ’93, стор. 218-232, 1993.
4. А. Янг, М. Юнг, «Клептографія: використання криптографії проти криптографії», Eurocrypt ’97, стор. 62-74, 1997.
5. А. Янг, М. Юнг, «Темна сторона криптографії чорної скриньки чи варто нам довіряти Capstone?», Crypto ’96, стор. 89-103.
6. С. Гольдвассер, С. Мікалі, «Імовірнісне шифрування», J. Comp. Sys. Sci. 28, с. 270-299, 1984.
7. Денін А. В. Криптографія. Практикум / А. В. Денін. — Харків : ХНУРЕ, 2020. — 128 с.
8. Семакин И. Г. Информатика: базовый курс / И. Г. Семакин, Е. К. Хеннер. — М. : Бином, 2018. — 352 с.
9. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис на основі еліптичної криптографії. — Чинний від 2003-01-01. — К. : Держспоживстандарт України, 2003. — 28 с.
10. RFC 6979. Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) [Електронний ресурс] / T. Pornin. — 2013. — Режим доступу: https://tools.ietf.org/html/rfc6979

11. Elliptic Curve Digital Signature Algorithm — Wikipedia [Електронний ресурс]. — 2024. — Режим доступу: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

12. Blockchain - ECDSA Algorithm — GeeksforGeeks [Електронний ресурс]. — 2023. — Режим доступу: https://www.geeksforgeeks.org/blockchain-elliptic-curve-digital-signature-algorithm-ecdsa/

13. Trail of Bits. ECDSA: Handle with care [Електронний ресурс]. — 2020. — Режим доступу: https://blog.trailofbits.com/2020/06/11/ecdsa-handle-with-care/

14. Mohamed M. A., Elkamchouchi H. M. Kleptographic attacks on elliptic curve signatures // International Journal of Computer Science and Network Security. — 2010. — Vol. 10, № 6. — P. 127–132.

15. Kovalenko A., Kudin A. Presentation: SETUP attacks and Kleptography [Електронний ресурс]. — 2020. — Режим доступу: PresentationKovalenko.pdf (з файлів наданих керівником)

16. Young A., Yung M. Kleptography: Using Cryptography Against Cryptography // EUROCRYPT 1997. Lecture Notes in Computer Science, vol. 1233. — Springer, 1997. — P. 62–74.

17. Certinal Blog. Understanding Digital Signatures [Електронний ресурс]. — 2023. — Режим доступу: https://www.certinal.com/blog/understanding-digital-signature