Розділ 3

МЕТОДИ ОЦІНКИ ТА ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ЕЦП З ДОДАТКОМ У ГРУПІ ТОЧОК ЕК

У розділах 1 і 2 цієї монографії розглянуто вимоги до ЕЦП, зроблено класифікацію та наведено достатньо повний опис існуючих ЕЦП. Особливістю застосування ЕЦП є те, що, як правило, дозволяється або рекомендується застосовувати національні, регіональні або міжнародні стандарти ЕЦП. Таким чином, вибір того чи іншого стандарту є обмеженим. Але на різних етапах створення й застосування ЕЦП необхідно вирішувати питання оцінки, порівняння та дослідження різних стандартів ЕЦП. Для розв'язання цих задач у виконаних на міжнародному рівні проектах оцінки та порівняння застосовувались методи експертних оцінок і, по суті, в подальшому голосування цих експертів і далі прийняття рішень щодо якості (ефективності) того чи іншого стандарту ЕЦП. Тому вважаємо актуальними задачі формалізації й автоматизації оцінок і порівняння стандартів застосовуваних ЕЦП.

На підтвердження указаного в цьому розділі наводяться результати досліджень та оцінок, пов'язаних з обґрунтуванням та вибором критеріїв і показників оцінки ЕЦП, досліджується стійкість ЕЦП як криптографічного перетворення відносно відомих атак і загроз, а також методики порівняння ЕЦП та результати їх застосування щодо ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичних кривих. При викладенні матеріалу ми орієнтуємось на основні опубліковані роботи, що є доступними [97–99]. Основна увага приділяється оцінці та дослідженню перш за все рівня криптографічної стійкості проти відомих на сьогоднішній день атак. Як результат наводяться методика та приклади оцінки й досліджень якості ЕЦП. Пропоновані методики ґрунтуються на двох (трьох) альтернативах. Вони наведені нижче у вигляді, що допускає їх практичну реалізацію та застосування. Нижче, у п. 3.1, наведено вибір та обґрунтування критеріїв і показників оцінки криптографічних перетворень типу ЕЦП, що ґрунтуються на еліптичних кривих. У своїй більшості наведені критерії та показники, на наш погляд, значною мірою можуть бути застосовані з деяким уточненням і для криптографічних перетворень типу «Направлене шифрування» і різних криптографічних протоколів. Причому ми розглядаємо декілька альтернативних варіантів існуючих систем критеріїв.

3.1. КРИТЕРІЇ ТА ПОКАЗНИКИ ОЦІНКИ ВЛАСТИВОСТЕЙ І ЯКОСТІ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ТИПУ ЕЦП, ЩО ҐРУНТУЮТЬСЯ НА ЕЛІПТИЧНИХ КРИВИХ

На світовому рівні ЕЦП вже набув дуже широкого розповсюдження в системах електронних документів та електронного документообігу, електронній пошті, платіжних системах, електронному врядуванні, електронній звітності, електронній торгівлі тощо. Зрозуміло, що при недостатньому рівні захищеності успішна реалізація загроз і атак може призвести до надзвичайно критичних ситуацій і подій, коли електронні документи та електронні дані будуть викривлені, підмінені, знищені тощо, особливо в процесі архівного зберігання значний час. Тому як дослідження, так і оцінка ЕЦП на різних етапах життєвого циклу ЕЦП – від розроблення до модифікації та виведення з дії, а також як наслідок застосування на різних етапах життєвого циклу даних є важливими задачами. Першими постають задачі визначення та вибору критеріїв і показників оцінки ЕЦП.

Під критерієм будемо розуміти ознаку, на основі якої здійснюється оцінка, визначення чи класифікація чого-небудь [173], тобто, по суті, будемо розуміти мірило оцінки. Попередні дослідження дозволили зробити висновок, що порівняння криптографічних кривих можна здійснити з використанням двох сукупностей критеріїв: безумовних та умовних [99, 109]. З урахуванням попереднього досвіду [99], оцінку криптоперетворень типу ЕЦП рекомендується виконувати у 2 етапи. На першому етапі перевіряється їх відповідність безумовним критеріям, а на другому отримуються відповідні оцінки з використанням умовних критеріїв. Саме за рахунок використання умовних критеріїв і з'являється можливість порівняти різні криптографічні перетворення типу ЕЦП за інтегральним критерієм.

Надалі під відповідністю безумовним критеріям будемо розуміти той факт, що експертні оцінки за безумовними критеріями є позитивними, тобто вони задовольняються (справджуються).

3.1.1. Безумовні критерії оцінки криптографічних перетворень типу ЕЦП, що ґрунтуються на еліптичних кривих

До безумовних критеріїв будемо відносити ті критерії, виконання яких для криптографічних перетворень типу ЕЦП в групі точок ЕК є обов'язковим, тобто безумовним.

Аналіз стану застосування [15, 16, 24, 27–37], досвід розроблення й оцінки властивостей криптоперетворень типу ЕЦП в групі точок ЕК [42–45, 52], досягнуті результати при практичному розв'язанні задач криптоаналізу та реалізації різних атак [7–9, 63, 64, 96–99] дозволяють як основні вибрати щонайменше такі безумовні критерії оцінки:

– надійність математичної бази, що застосовується для ЕЦП при криптоперетвореннях;

– практична захищеність криптографічних перетворень типу ЕЦП від відомих атак;

– реальна захищеність ЕЦП від усіх відомих та потенційно можливих криптоаналітичних атак;

– статистична безпечність криптографічного перетворення типу ЕЦП в групі точок еліптичної кривої;

– теоретична захищеність криптографічного перетворення типу ЕЦП в групі точок еліптичної кривої;

– відсутність слабких особистих ключів криптографічного перетворення типу ЕЦП в групі точок еліптичної кривої;

– складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень у групі точок еліптичної кривої щодо ЕЦП має не вище за поліноміальний характер.

Розглянемо більш детально ці критерії як щодо понять і визначень, так і щодо особливостей застосування.

1. Надійність математичної бази, у розумінні відсутності в порушника можливостей здійснювати атаки типу «Універсальне розкриття» за рахунок недосконалості математичної бази групи точок еліптичних кривих або слабкостей, що можуть бути закладені за рахунок специфічних властивостей загальних параметрів і ключів. При цьому критерієм оцінки надійності математичної бази є той факт, що складність атаки «Універсальне розкриття» $I_{ур}$ має експоненційний характер, а критерієм ненадійності – субекспоненційний або поліноміальний характер складності. Будемо позначати цей критерій $W_{\delta 1}$.

2. Практична захищеність криптоперетворень у групі точок ЕК від силових і аналітичних атак, яка досягається за рахунок вибору розмірів загальних параметрів і ключів. Тобто критерієм практичної захищеності криптоперетворень типу ЕЦП є вибір таких розмірів загальних параметрів і ключів, за яких складність атаки $I_{са}$ суттєво (на необхідне число порядків) перевищує існуючу потужність криптоаналітичних систем на рівні технологічно розвинутих держав (порушника третього рівня), у тому числі з урахуванням прогнозу збільшення потужності криптоаналітичних систем за рахунок розвитку математичного та програмного забезпечення, а також апаратних і програмно-апаратних засобів. Позначимо цей безумовний критерій $W_{\delta 2}$.

3. Реальна захищеність від усіх відомих і потенційно можливих криптоаналітичних атак, де під захищеністю розуміють той факт, що всі відомі криптоаналітичні атаки типу «Повне розкриття» мають експонентну складність $I_{ес}$, а під критерієм незахищеності – субекспоненційний $I_{се}$ і нижче характер складності атаки «Повне розкриття». Будемо позначати цей безумовний критерій $W_{\delta 3}$.

4. Статистична безпечність криптографічного перетворення типу ЕЦП в групі точок еліптичної кривої, під якою розуміють статистичну незалежність результату криптографічного перетворення (виходу), наприклад самого ЕЦП (криптограми), від вхідного блоку, що зашифровується (підписується), та особистого ключа, що використовується. Будемо позначати цей безумовний критерій $W_{\delta 4}$.

5. Теоретична захищеність криптографічного перетворення типу ЕЦП, у якому використовуються загальні параметри з відповідними властивостями та довжинами, для якого не існують (невідомі) теоретичні аналітичні атаки, складність яких менша, ніж складність атаки типу «Повне розкриття». Цей безумовний критерій будемо позначати $W_{\delta 5}$.

6. Відсутність слабких особистих ключів, за яких складність криптоаналітичних атак типу «Повне розкриття» та «Універсальне розкриття» є меншою, ніж складність атаки «Повне розкриття» для інших (не слабких) особистих ключів. Позначимо цей безумовний критерій як $W_{\delta 6}$.

7. Складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень має поліноміальний характер і не перевищує допустимих величин $I_{пр}'$ та $I_{фв}'$. Позначимо цей безумовний критерій також $W_{\delta 7}$.

Оскільки наведені часткові критерії є безумовними, то критерієм добору є логічна зміна так/ні (1/0), тому безумовний критерій можна записати у вигляді:

$$(K_{\delta 1}, K_{\delta 2}, K_{\delta 3}, K_{\delta 4}, K_{\delta 5}, K_{\delta 6}, K_{\delta 7}) \in (1,0). \quad (3.1)$$

З урахуванням наведених вище часткових безумовних критеріїв $W_{\delta 1}$–$W_{\delta 7}$ та умови (3.1) функцію відповідності криптоперетворення в групі точок еліптичних кривих може бути записано у вигляді:

$$f_{фв}() = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5} \wedge W_{\delta 6} \wedge W_{\delta 7}. \quad (3.2)$$

Де символ «∧» позначає операцію кон'юнкції булевих змінних.

Таким чином, якість криптографічного перетворення в групі точок еліптичних кривих може бути оцінена з використанням безумовного інтегрального критерію – функції відповідності криптоперетворення вимогам $f_{фв}() \in (0; 1)$ та при $f_{фв}() = 1$ криптографічне перетворення в групі точок ЕК, що оцінюється, відповідає вимогам.

Запропонований інтегральний критерій дозволяє тільки встановити, чи відповідає встановленим вимогам криптоперетворення типу ЕЦП, що розглядається.

3.1.2. Умовні критерії оцінки криптографічних перетворень типу ЕЦП з додатком, що ґрунтуються на еліптичних кривих

Якісне й кількісне порівняння криптографічних перетворень в групі точок ЕК можна здійснити, використовуючи узагальнений критерій переваги [99, 109].

Як основні складові узагальненого критерію переваги пропонується використовувати такі часткові умовні критерії (табл. 3.1).

Таблиця 3.1. **Умовні критерії оцінки криптоперетворень**

Критерії	Позначення
Можливість і умови вільного поширення та застосування міжнародного чи національного стандарту криптографічних перетворень типу ЕЦП в групі точок еліптичних кривих в Україні з урахуванням вимог нормативно-правових актів України на експорт, імпорт і обмеження на його застосування	K_{y1}
Рівень довіри до міжнародного чи національного стандарту криптографічного перетворення типу ЕЦП в групі точок еліптичних кривих на різних рівнях застосування	K_{y2}
Перспективність застосування міжнародного гармонізованого чи національного стандарту ЕЦП в Україні	K_{y3}
Часова і просторова складності програмної, програмно-апаратної та апаратної реалізацій вироблення й перевіряння ЕЦП	K_{y4}

Продовження табл. 3.1

Критерії	Позначення
Можливість та умови застосування відповідного стандарту ЕЦП з різними загальними параметрами та в різних режимах	K_{y5}
Гнучкість стандарту криптографічного перетворення типу ЕЦП в групі точок еліптичних кривих з точки зору застосування в різних додатках і при різних реалізаціях засобів	K_{y6}
Рівень захищеності ЕЦП при здійснені різних видів загроз у різних умовах апріорної та апостеріорної визначеності, у тому числі при відхиленні від вимог або порушенні властивостей загальних параметрів	K_{y7}

3.1.3. Показники оцінки якості криптоперетворень типу ЕЦП з додатком в групі точок ЕК

Надалі оцінку за кожним із часткових безумовних і умовних критеріїв будемо здійснювати, використовуючи множину показників, що підтримують заданий критерій.

Розглянемо спочатку основні показники, за якими можна оцінити стандарти криптографічних перетворень у групі точок ЕК за безумовними критеріями.

Оцінку надійності математичної бази можна здійснити на основі експертних оцінок спеціалістів у галузі криптології. При цьому має враховуватись ступінь відкритості проектування та дослідження стандарту або взагалі криптографічного перетворення типу ЕЦП. Важливим же фактором є можливість або підозра на її існування в частині моделювання криптоперетворень та виконання криптоаналізу зі зменшеною або суттєво зменшеною складністю. Основним же показником оцінки надійності математичної бази криптоперетворень у групі точок ЕК може бути використано ступінь погіршення безпечного часу

$$r_н = \frac{t_б}{t'_б},$$

де $t_б$ – математичне сподівання часу криптоаналізу для дійсного математичного перетворення, а $t'_б$ – для моделювального математичного апарату.

На основі експертних оцінок приймається рішення. Якщо $r_н > 1$, то з урахуванням експертних оцінок може бути прийнято рішення, що $W_{б1} = 0$, інакше $W_{б1} = 1$.

Практичну захищеність криптографічних перетворень у групі точок ЕК від силових атак будемо оцінювати орієнтуючись на розмір особистого ключа. Під силовою атакою будемо розуміти направлений перебір особистих ключів d_i та/або ключів сеансу (параметрів) k_j. Оскільки d_i та k_j повинні формуватись випадково, рівноймовірно та незалежно і $0 < d_i, k_j < n$, де n – порядок базової точки G, то ймовірність підбору з однієї спроби $P(1)$ можна оцінити, якщо відоме число n, тобто порядок базової точки n, у бітах:

$$P(1) \geq \frac{1}{n} = \frac{1}{2^m} = 2^{-m}.$$

У k спробах імовірність підбору $P(k)$ можна обчислити як

$$P(k) = \frac{k}{n} = \frac{k}{2^m} = k2^{-m} \cdot \tag{3.3}$$

Оцінку складності силової атаки можна зробити способом оцінки складності виконання атаки I_d та безпечного часу $t_б$. Для умови, коли $0 < d_i, k_j < n$, складність можна оцінити як

$$I_d = n = 2^m, \tag{3.4}$$

а безпечний час

$$t_б = \frac{I_d}{\gamma K} P_y, \tag{3.5}$$

де γ – потужність криптоаналітичної системи, $K = 3{,}15 \cdot 10^7$ сек/рік, P_y – ймовірність, з якою повинен чи може бути успішно здійснений криптоаналіз.

На основі аналізу стану практичної захищеності приймається рішення, що $W_{б2} = 1$ або $W_{б2} = 0$.

Реальну захищеність криптоперетворень у групі точок еліптичної кривої пропонується оцінювати визначенням складності I_a та безпечного часу $t_б$ здійснення атаки типу «Повне розкриття» для i-го методу криптоаналізу. Детально ці оцінки наведено в розділі 4 цієї книги (монографії). Наприклад, якщо розв'язання дискретного логарифмічного рівняння в групі точок еліптичної кривої здійснюється ρ-методом Полларда [64, 96, 99, 115], то складність і безпечний час з допустимою точністю можна визначити як

$$I_{a_ρ} \approx \sqrt{\frac{\pi n}{4}}, \tag{3.6}$$

$$t_{б_ρ} = \frac{I_{a_ρ}}{\gamma K} P_y = \frac{\sqrt{\pi n}}{2\gamma K} P_y. \tag{3.7}$$

Значення $I_{a_ρ}$ та $t_{б_ρ}$ визначаються для всіх методів криптоаналізу. Якщо вони мають експоненційний характер, то захищеність криптоперетворень оцінюється як така, що відповідає вимогам. Якщо вони мають субекспоненційний характер, то захищеність криптоперетворення типу ЕЦП оцінюється як така, що не відповідає вимогам.

Окрім того, навіть при експонентному характері, у разі розгляду різних методів розв'язку дискретного логарифмічного рівняння в групі точок ЕК реальну захищеність пропонується оцінювати як

$$I_a = \min\left(I_{a1}, I_{a2}, \ldots, I_{ak}\right), \tag{3.8}$$

$$t_б = \min\left(t_{б1}, t_{б2}, \ldots, t_{бk}\right). \tag{3.9}$$

Тобто пропонується оцінювати за найменшим (найгіршим) значенням складності криптоаналізу.

На основі оцінки реальної захищеності приймається рішення, що $W_{б3} = 1$ або $W_{б3} = 0$.

Для блокового криптоперетворення, яким є перетворення типу ЕЦП в групі точок ЕК, необхідно також оцінювати ймовірність виникнення колізій.

У [7, 12, 51, 95] запропоновані підходи до оцінки ймовірності виникнення колізій для блокових симетричних шифрів і функцій гешування. Особливістю криптоперетворення типу ЕЦП є те, що результатом перетворення є точка і по суті треба розглядати питання колізії точок. Проведений аналіз показав, що ця задача теоретичного й практичного розгляду та розв'язання в частині ЕЦП ще не знайшла. Але вона може бути вирішена при відповідному обґрунтуванні та визначенні порядку базової точки n засобом застосування уже стандартного методу на основі парадоксу про день народження [7, 51].

Окрім того, проведений аналіз показав, що відносно криптоперетворень у групі точок еліптичних кривих на сьогодні методи та підходи оцінки статистичної безпечності не розвинуті. Їх обґрунтування та вибір являють собою окрему задачу. З урахуванням підходів і пропозицій [7, 51, 95, 96] та враховуючи блочний характер криптоперетворень, попередню оцінку статистичної безпечності пропонується виконувати визначенням математичного сподівання та дисперсії функції взаємної кореляції. Спочатку визначаємо функцію взаємної кореляції між входом M_i та виходом C_i:

$$F_1 = f(M_i, C_i) = \sum_{j=1}^{l} M_{ij} \oplus C_{ij}. \tag{3.10}$$

Окрім того, будемо визначати функцію взаємної кореляції між виходами (криптограми) для різних ключів і блоків повідомлень:

$$F_2 = f(C_i, C_k) = \sum_{j=1}^{l} C_{ij} \oplus C_{kj}. \tag{3.11}$$

Далі, розглядаючи значення F_1 та F_2 як випадкові, обчислюємо математичне сподівання $m_1(F_1)$ і $m_1(F_2)$, а також дисперсію $m_2(F_1)$ і $m_2(F_2)$.

Рішення будемо приймати таким чином. Блок інформації M_i та блок-криптограма C_i є залежними, якщо $m_1(F_1)$ і $m_2(F_1)$ є параметрами біноміального розподілу. Аналогічно рішення приймається й щодо C_i та C_k. Криптограми за будь-яких M_i, M_k та K_i, K_j можна вважати незалежними, якщо відповідні $m_1(F_2)$ і $m_2(F_2)$ також є параметрами біноміального розподілу.

Іншим, допустимим способом оцінки статистичної безпечності є визначення надмірності й залежності символів криптограм. У цьому випадку оцінку можна здійснити як

$$k_2 = \frac{l'_c}{l_c}, \tag{3.12}$$

де l'_c – довжина стиснутого блоку криптограми, l_c – довжина блоку криптограми.

Рішення в цьому випадку приймається на основі аналізу k_2, що ближче k_2 до 1, то кращою вважається статистична безпечність, оскільки блок-криптограма все більше стає схожою на випадкову послідовність.

У цілому, на основі одержаних результатів та оцінок робиться висновок про статистичну безпечність алгоритму криптоперетворення в групі точок ЕК і $W_{\delta 4} = 1$ або $W_{\delta 4} = 0$.

Оцінку теоретичної захищеності криптоперетворень у групі точок ЕК пропонується роботи на основі визначення наявності, підозри на наявність чи відсутність теоретичних аналітичних атак.

Ця оцінка може бути здійснена на основі експертних оцінок спеціалістів-криптологів. Під час оцінки експерти мають враховувати сферу застосування стандарту (наприклад, електронний цифровий підпис, направлене шифрування, криптографічний протокол тощо), можливі загрози (наприклад, у вигляді атаки «Повне розкриття», «Універсальне розкриття» тощо). Підозра на наявність загрози у вигляді теоретичних атак, якщо складність цих атак має субекспоненційний характер або можливі інші вразливості, що не дозволять гарантувати необхідну криптографічну стійкість. Основними показниками при цьому є складність теоретичної криптоаналітичної атаки, безпечний час (час її здійснення) та ймовірність здійснення аналітичної атаки. Відповідні показники наведені вище при оцінці реальної захищеності криптоперетворення в групі точок ЕК (формули 3.6–3.9).

Таким чином, якщо складність можливої теоретичної атаки має субекспоненційний характер і ймовірність її здійснення $P_{ат} > P_{доп}$, то приймається рішення, що $W_{\delta 5} = 0$, інакше $W_{\delta 5} = 1$.

Проведений аналіз показав, що пошук слабких особистих ключів або відкритих ключів, для яких атаки типу «Повне розкриття» чи «Універсальне розкриття» мають субекспоненційний характер, є дуже складною задачею.

Першою причиною слабкості може стати засіб або система генерування ключів. Зрозуміло, що особисті ключі повинні формуватись (генеруватись) випадково, рівноймовірно та незалежно. Для забезпечення цих властивостей необхідно використовувати фізичні джерела «білого» шуму. Але й у цьому випадку щільність розподілу та його характеристики можуть бути викривленими в результаті наявності у фізичного генератора ε-асиметрії, коли ймовірності $P(1)$ та $P(0)$ різняться між собою. Наприклад, $P(1) = 0{,}5 + \varepsilon$, а $P(0) = 0{,}5 - \varepsilon$. Наявність достатньої ε-асиметрії дозволяє зменшити складність атаки «груба сила», яка в цьому випадку може здійснюватись з урахуванням зсуву розподілу, коли змінюється ймовірність появи ключа з даним співвідношенням між «1» та «0». Тому першим кроком є пред'явлення до джерела ключів вимог щодо допустимої величини ε, наприклад, $\varepsilon \le 10^{-5}$. Ця вимога може бути виконана за рахунок використання фізичних джерел шуму та генераторів випадкових послідовностей, що будуються на основі цих джерел, а також коли $\varepsilon < \varepsilon_{доп}$.

Таким чином, під час аналізу ключів у першу чергу необхідно проаналізувати джерело ключів та обмежити допустиму величину ε-асиметрії.

Слабкими необхідно також вважати ключі $d_i(k_i)$, при використанні яких зменшується складність розв'язання дискретного логарифмічного рівняння в групі точок еліптичних кривих. Слабкими, очевидно, також необхідно вважати такі ключі, ймовірність появи яких є занадто малою та які можуть з'являтись у результаті появи несправностей.

Таким чином, наявність або підозри на наявність слабких ключів, а також еквівалентних ключів, мають бути встановлені експертами-криптологами. Якщо слабкі ключі при цьому в системі блокуються і стійкість через це не зменшується, то такий стандарт можна вважати таким, що його алгоритм не має слабких ключів. У цьому випадку безумовний критерій $W_{\delta 6} = 1$, інакше $W_{\delta 6} = 0$.

Складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень може оцінюватись як теоретично так і експериментально. Експериментальна

оцінка може бути здійснена з використанням відповідних засобів, що реалізують перетворення: програмних, програмно-апаратних та апаратних. При цьому оцінка може проводитись засобом вимірювання швидкості виконання тих чи інших операцій. Просторову складність I_v можна оцінити через об'єм пам'яті, необхідний для виконання прямих і зворотних перетворень у групі точок еліптичних кривих, розміщення ключів, таблиць, параметрів і сертифікатів. Якщо при цьому $I_v \le I_v^{доп}$, то експерт приймає рішення, що $W_{\delta 7} = 1$, інакше $W_{\delta 7} = 0$.

Далі, залежно від вимог до складності прямого $I_{пр}$ та зворотного $I_{зв}$ перетворень, експерт приймає рішення, що $W_{\delta 7} = 1$, якщо складність перетворень не перевищує допустимих значень, і $W_{\delta 7} = 0$ – якщо перевищує.

Таким чином, на основі аналізу часової та просторової складності криптографічних перетворень у групі точок еліптичних кривих експерти приймають рішення за безумовним критерієм (3.2).

3.1.4. Показники та порядок оцінки ЕЦП з додатком у групі точок еліптичних кривих методом ієрархій

Досвід рішення такого класу задач, накопичений при виконанні проектів AES [174] та NESSIE [175], а також з урахуванням [175] дозволяє запропонувати підхід, що ґрунтується на використанні математичного апарату нечітких множин.

На сьогоднішній день не існує систематизованого підходу для перетворення множини значень показників у єдиний показник, яким можна схарактеризувати ефективність функціонування схеми криптографічного перетворення. Як відзначено раніше, розробники криптографічних стандартів пропонують різні набори показників, що характеризують окремі сторони шифрів, але це не дозволяє уявити картину в цілому. Однак для вирішення таких задач на практиці застосовуються елементи теорії нечітких множин. Розглянемо основні елементи цієї теорії [109, 176].

Нехай U – повна множина, що охоплює всі об'єкти деякого класу. Нечітка підмножина F множини U, що її надалі будемо називати нечіткою множиною, визначається через функцію приналежності $\mu_F(u)$, $u \in U$. Ця функція відображає елементи u_i множини U на множину ірраціональних чисел відрізка [0,1], що вказують ступінь приналежності кожного елемента нечіткій множині F.

Якщо повна множина U складається з кінцевого числа елементів u_i, $i = 1, 2, ..., n$, то нечітку множину F можна подати в такому вигляді:

$$F = \mu_F(u_1)/u_1 + \mu_F(u_2)/u_2 + ... + \mu_F(u_n)/u_n, \qquad (3.13)$$

де знак «+» означає не додавання, а об'єднання;

символ «/» показує, що значення μ_F належить до елемента, який іде за ним (а не означає ділення на u_i).

Таким чином, для вирішення задачі вибору криптографічного перетворення в групі точок ЕК можна скористатися елементами теорії нечітких множин. Експертні оцінки альтернативних варіантів за визначеними нами умовними крите-

ріями можуть бути подані як нечіткі множини або числа, виражені за допомогою функцій приналежності. Для упорядкування нечітких чисел існує безліч методів, що відрізняються один від іншого способом згортки та побудови нечітких відносин. Останнє можна визначити як відносини переваги між об'єктами. Розглянемо одну з математичних постановок задачі прийняття рішень на основі теорії нечітких множин [176].

У цьому випадку критерії визначають деякі поняття, а оцінки альтернатив являють собою ступені відповідності цим поняттям. Нехай є множина альтернатив $A = \{a_1, a_2, ..., a_m\}$ і множина критеріїв $C = \{C_1, C_2, ..., C_n\}$, при цьому оцінки альтернатив за кожним *i-м* критерієм подані нечіткими множинами:

$$C_i = \{\mu_{C_i}(a_1)/a_1 + \mu_{C_i}(a_2)/a_2 + ... + \mu_{C_i}(a_m)/a_m\}. \quad (3.14)$$

Правило вибору кращої альтернативи можна подати як перетинання нечітких множин, що відповідають критеріям:

$$D = C_1 \cap C_2 \cap ... \cap C_n. \quad (3.15)$$

Операція перетинання нечітких множин може бути реалізована різними способами. Іноді перетинання виконується як множення, але зазвичай цій операції відповідає взяття мінімуму:

$$\mu_D(a_j) = \min_{i=1,...,n} \mu_{C_i}(a_j), j = 1,...,m \quad (3.16)$$

Кращою вважається альтернатива a^*, що має найбільше значення функції приналежності:

$$\mu_D(a^*) = \max_{j=1,...,m} \mu_D(a_j). \quad (3.17)$$

У нашому випадку всі критерії мають різну важливість, тому їх внесок у загальне рішення можна подати як зважене перетинання:

$$D = C_1^{\beta_1} \cap C_2^{\beta_2} \cap ... \cap C_n^{\beta_n}, \quad (3.18)$$

де β_i – вагові коефіцієнти відповідних критеріїв, що повинні задовольняти умовам:

$$\beta_i \geq 0; \quad i = 1,...,n; \quad (1/n)\sum_{i=1}^{n} \beta_i = 1. \quad (3.19)$$

Коефіцієнти відносної важливості визначаються з використанням процедури попарного порівняння критеріїв.

Розглянемо цю процедуру, використовуючи метод попарного порівняння.

Метод попарного порівняння елементів [176] можна описати в такий спосіб. Будується множина матриць парних порівнянь. Парні порівняння проводяться в термінах домінування одного елемента над іншим. Отримані судження виражаються в цілих числах з урахуванням дев'ятибальної шкали [див. табл. 3.2].

Таблиця 3.2. **Шкала відносин (ступеня значимості дій)**

Ступінь значимості	Визначення	Пояснення
1	Однакова значимість	Дві дії роблять однаковий внесок у досягнення мети
3	Деяка перевага значимості однієї дії над іншою (слабка значимість)	Існують свідчення на користь переваги однієї з дій, однак вони недостатньо переконливі
5	Істотна або сильна значимість	Є надійні дані або логічні судження для того, щоб показати перевагу однієї з дій
7	Очевидна або дуже сильна значимість	Переконливе свідчення на користь однієї дії перед іншою
9	Абсолютна значимість	Свідчення на користь переваги однієї дії щодо іншої найвищою мірою переконливі
2, 4, 6, 8	Проміжні значення між двома сусідніми судженнями	Ситуація, коли необхідне компромісне рішення
Зворотні величини наведених вище ненульових величин	Якщо дії i при порівнянні з дією j приписується одне з визначених вище ненульових чисел, то дії j при порівнянні з дією i приписується зворотне значення	Якщо узгодженість була постульованою при одержанні N числових значень для утворення матриці

Правомірність цієї шкали доведена теоретично при порівнянні з багатьма іншими шкалами [176]. При використанні зазначеної шкали ЛПР, порівнюючи два об'єкти в сенсі досягнення мети, розташованої на вищому рівні ієрархії, повинний поставити у відповідність цьому порівнянню число в інтервалі від 1 до 9 або зворотне значення чисел. У тих випадках, коли важко розрізнити стільки проміжних градацій від абсолютної до слабкої переваги або цього не потрібно в конкретній задачі, може використовуватися шкала з меншим числом градацій. У границі шкала має дві оцінки: 1 – об'єкти рівнозначні; 2 – перевага одного об'єкта над іншим.

Заповнення квадратних матриць парних порівнянь здійснюється за таким правилом. Якщо елемент E_1 домінує над елементом E_2, то клітка матриці, що відповідає рядку E_1 і стовпцю E_2, заповнюється цілим числом, а клітка, що відповідає рядку E_2 і стовпцю E_1, заповнюється зворотним йому числом. Якщо елемент E_2 домінує над E_1, то ціле число ставиться в клітку, що відповідає рядку E_2 і стовпцю E_1, а дріб проставляється в клітку, що відповідає рядку E_1 і стовпцю E_2. Якщо елементи E_1 і E_2 рівно домінують, то в обох позиціях матриці ставляться одиниці.

Для одержання кожної матриці експерт або ЛПР виносить $n(n-1)/2$ суджень (тут n – порядок матриці парних порівнянь).

Розглянемо в загальному вигляді приклад формування матриці парних порівнянь.

Нехай $E_1, E_2, ..., E_n$ – множина з n елементів (альтернатив) і $v_1, v_2, ..., v_n$ – відповідно їх ваги, або інтенсивності. Порівняємо попарно вагу або інтенсивність кожного елемента з вагою або інтенсивністю будь-якого іншого елемента множини стосовно загальної для них властивості чи мети. У цьому випадку матриця парних порівнянь $[E]$ має такий вигляд:

		E_1	E_2	...	E_n
E_1		v_1/v_1	v_1/v_2	...	v_1/v_n
$[E] =$	E_2	v_2/v_1	v_2/v_2	...	v_2/v_1
	...	...	...	...	...
E_n		v_n/v_1	v_n/v_2	...	v_n/v_n

При проведенні попарних порівнянь варто відповідати на такі питання: який із двох порівнюваних елементів важливіше або має більший вплив, який більш імовірний і який кращий. При порівнянні критеріїв зазвичай запитують, який із критеріїв більш важливий; при порівнянні альтернатив стосовно критерію – яка з альтернатив краща чи більш імовірна [176].

Ранжирування елементів, що аналізуються з використанням матриці парних порівнянь $[E]$, здійснюється на підставі головних власних векторів, що одержують у результаті обробки матриць.

Обчислення головного власного вектора W позитивної квадратної матриці $[E]$ проводиться на підставі рівності

$$EW = \lambda_{max} W, \tag{3.20}$$

де λ_{max} – максимальне власне значення матриці $[E]$.

Для позитивної квадратної матриці $[E]$ правий власний вектор W, що відповідає максимальному власному значенню λ_{max}, з точністю до постійного співмножника C можна обчислити за формулою:

$$\lim_{k\to\infty} \frac{[E]^k e}{e^T [E]^k e} = CW, \tag{3.21}$$

де $e = \{1,1, ...,1\}^T$ – одиничний вектор;

$k = 1, 2, 3, ...$ – показник ступеня;

C – константа;

T – знак транспонування.

Обчислення власного вектора W згідно з (3.20) здійснюється до досягнення заданої точності:

$$e^T \mid W^{(l)} - W^{(l+1)} \mid \leq \xi, \tag{3.22}$$

де l – номер ітерації – такий, що $l = 1$ відповідає $k = 1$; $l = 2$, $k = 2$; $l = 3$, $k = 4$ і т.д.;

ξ – припустима похибка (з достатньою для практики точністю можна прийняти $\xi = 0{,}01$ незалежно від порядку матриці).

Максимальне власне значення матриці обчислюється за формулою:

$$\lambda_{\max} = e^T [E] W. \tag{3.23}$$

Запропонований підхід дозволяє порівняти різні суб'єкти, наприклад, стандарти криптографічних перетворень за узагальненим умовним критерієм і одержати кількісне значення оцінки, визначити перевагу одного над іншим. Повністю методика порівняльного аналізу ЕЦП з додатком і приклад порівняльного аналізу наведено в 3.8.1.

3.2. ОЦІНКА КРИПТОГРАФІЧНОЇ СТІЙКОСТІ ЕЦП В ГРУПІ ТОЧОК ЕК ВІД АТАК ТИПУ «ПОВНЕ РОЗКРИТТЯ»

3.2.1. Огляд методів розв'язання дискретного логарифма в групах точок на еліптичних кривих

Розглянемо у відповідності з (1.1) проблему розв'язання дискретного логарифма на еліптичних кривих. Нехай є точки ЕК $Q, G \in E(F(q))$, необхідно вирішити рівняння $Q = d \cdot G$ відносно особистого ключа d або довести, що рішення не існує. Необхідна умова, що має бути виконана:

$$Q \in \langle G \rangle, \text{ тобто } d \in [1, ordG - 1 = n], \text{ значить } n \cdot G = 0,$$

де G – базова точка, що формує групу;

n – порядок базової точки $n = ordG$;

Q – відкритий ключ;

0 – точка нескінченності;

операція «·» означає скалярне множення на еліптичній кривій.

Залежно від вхідних даних задачу розв'язання дискретного логарифмічного рівняння можна розглядати з такими формулюваннями [7–9, 64, 96].

Відомий порядок базової точки $ordG = n$, також відомо, що особистий (таємний) ключ d обраний випадково з інтервалу $d \in [1, ordG]$, причому відкритий ключ Q_A зв'язаний з особистим через базову точку, тобто

$$Q_A = d_A \cdot G (\bmod q), \tag{3.24}$$

над довільним простим полем Галуа з модулем q.

Також параметри еліптичної кривої a та b мають задовольняти умові:

$$4a^3 + 27b^2 \neq 0 \ (\bmod P). \tag{3.25}$$

Ця стандартна задача знаходження особистого ключа d способом розв'язання дискретного логарифма в групі точок еліптичної кривої.

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з невідомим порядком

У випадку коли, наприклад, точка Q – точка нескінченності O_E, під знаходженням $d = \log_G Q$ розуміють знаходження порядку базової точки G. У цьому випадку точно не відомий порядок базової точки $ordG = n$, але замість цього відомі деякі відомості про d. Наприклад, можуть бути відомі множники d, точна кількість бітів у старших і молодших розрядах, наближення або ймовірнісний розподіл d.

За таких умов задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій [96] може бути виконана в такій постановці й за таких умов.

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомим інтервалом

Нехай a та b – цілі числа $0 \le a < b$, $d \in [a,b]$. Така задача припускає розв'язання рівняння $Q = d \cdot G$ з відомими a, b, G. Якщо $a = 1$ і $b = ordG$, задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомим інтервалом $[a,b]$ стає стандартною задачею розв'язання дискретного логарифмічного рівняння на еліптичній кривій. Причина вибору секретного ключа d такого спеціального виду може полягати в тому, що скалярне множення точки на еліптичній кривій $G \cdot d$ буде швидше, ніж для випадково обраного d.

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомим інтервалом $[a,b]$ може бути вирішена за час $O(\sqrt{b-a})$ із просторовою складністю $O(\sqrt{b-a})$, або з очікуваним часом $O(\sqrt{b-a})$ з постійною просторовою складністю [159].

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомою вагою Хеммінга

Якщо $\mu = \lceil \log_2(ordG) \rceil$, то двійкове подання $d = \log_G Q$ вимагає максимально μ бітів, та ми можемо записати d у вигляді $d = \sum_{i=0}^{\mu-1} d_i 2^i$, де $d_i \in \{0,1\}$ для $0 \le i \le \mu - 1$. Кількість одиниць у такому поданні називається *вагою Хеммінга* і позначається $wt(x)$. Нехай $t < \mu$ таке, що $wt(d) = t$, тоді розв'язання $Q = G \cdot d$ відносно d з вихідними даними μ, t, G називається задачею розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомою вагою Хеммінга. Можливість застосування такої атаки обумовлена тим, що швидкість скалярного множення числа на точку еліптичної кривої перебуває в прямій залежності від t: що менше вага Хеммінга, то скоріше виконується скалярне множення.

Ця задача може бути вирішена за час

$$O\left(\mu\binom{\mu/2}{\mu/2}\right) \tag{3.26}$$

із просторовою складністю

$$O\left(\mu\binom{\mu/2}{\mu/2}\right), \tag{3.27}$$

або очікуваний час

$$O\left(\sqrt{t}\binom{\mu/2}{\mu/2}\right) \tag{3.28}$$

із необхідною просторовою складністю

$$O\left(\frac{\mu/2}{\mu/2}\right) \text{[63]}. \qquad (3.29)$$

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з рішенням, що лежить у деякому класі

Нехай q – ціле число, $2 \le q < ordG$. Нехай a, q та d будуть такими, що $d \equiv a \bmod q$. Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з рішенням, що лежить у деякому відомому класі – це задача розв'язання рівняння $Q = d \cdot G$ відносно особистого ключа d з відомими вхідними даними a, q, G. Якщо порядок базової точки відомий і $q \le ord\, G$, то ця задача зводиться до задачі розв'язання дискретного логарифмічного рівняння на еліптичній кривій з відомим інтервалом $[a, b]$.

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій з рішенням, що лежить у деякому відомому класі може бути вирішена (приблизно) за час $O\left(\sqrt{ordG/q}\right)$ [96].

Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій за відомого ймовірнісного розподілу

Нехай $p_0, p_1, \ldots$ будуть не негативними реальними числами, такими що $\sum_{i=0}^{\infty} p_i = 1$. Припустимо, що $Q = G \cdot d$, де d обрано випадково з імовірнісним законом розподілу (p_i), де $p_i = prob(x = i)$. Задача розв'язання дискретного логарифмічного рівняння на еліптичній кривій за відомого ймовірнісного розподілу – це задача розв'язання $Q = G \cdot d$ відносно d з відомими значеннями (p_i), G та Q. Якщо $p_i = 1/ordG$ для $1 \le i \le ordG$, то задачу розв'язання дискретного логарифмічного рівняння на еліптичній кривій за відомого ймовірнісного розподілу можна звести до стандартної задачі розв'язання дискретного логарифмічного рівняння на еліптичній.

У додатку Б (на диску) наведено огляд існуючих методів вирішення дискретного логарифмічного рівняння в групі точок еліптичних кривих.

Наведені методи розв'язання дискретного логарифму в групі точок ЕК відносно особливостей виконання й точності результату можна розділити на такі два великих класи:

1) ***детерміновані*** (точні) – алгоритми, які використовують стратегію пошуку, що дає точне рішення;

2) ***імовірнісні*** – алгоритми, які використовують імовірнісну стратегію пошуку, що впливає на час пошуку рішення.

Попередній аналіз указаних методів дозволив зробити висновки, що найменшою складністю володіють методи ρ-Полларда та λ-Полларда. Тому в наступних параграфах розглянемо та порівняємо їх детально.

3.2.2. ρ-метод Полларда розв'язання дискретного логарифмічного рівняння в групі точок еліптичних кривих

Розглянемо детально ρ-метод Полларда, що реалізує атаку типу «Повне розкриття» [96]. Основним завданням такої атаки є визначення особистого ключа d користувача (власника). При цьому приймемо, що атака здійснюється за таких

умов. Відомі методи, алгоритми й протоколи виконання узгодження ключів або іншого протоколу, що використовує скалярне множення на еліптичних кривих. Криптоаналітик має доступ та знає системні параметри, базову точку, її порядок і відкриті ключі.

Відоме також рівняння, що використовується для обчислення відкритих ключів [1–3, 5, 6] за особистим виглядом (3.24), яке для загального випадку будемо подавати в такому вигляді:

$$Q = kG \,(\mathrm{mod} f(x), p), \tag{3.30}$$

де $k = d$, або $k = -d$, або $k = d^{-1}$;

d – особистий ключ;

G – значення базової точки порядку n;

$f(x)$ – примітивний поліном над полем $GF(p^m)$.

Іншою аналогічною задачею є задача Діффі-Геллмана [7, 51, 63, 96], що формулюється в такому вигляді. Відомі відкриті ключі, наприклад, обчислені з використанням формул:

$$Q_1 = k_1 G, \quad Q_2 = k_2 G.$$

Завданням криптоаналітика є знаходження спільної таємниці, що використовується для встановлення (узгодження) спільного ключа

$$K_{12} = K_{21} = d_1 d_2 G \,(\mathrm{mod} f(x), p). \tag{3.31}$$

Розв'язанню розглянутих вище задач «повного розкриття» присвячене значне число робіт, результати аналізу яких наведено в додатку Б (на диску). Аналіз зазначених робіт показує, що атака типу «Повне розкриття» повинна здійснюватися в такій послідовності. Криптоаналітик здобуває або перехоплює реальні діючі значення системних параметрів і значення відкритого ключа. Далі, використовуючи найбільш швидкий (ефективний метод) вирішується задача визначення особистого ключа d з рівняння (3.25). При цьому якщо час, витрачений на розв'язання задачі дискретного логарифмування, менше терміну дії ключа d, то в подальшому криптоаналітик може вирішувати задачі порушення цілісності, конфіденційності, спостережливості й доступності в інтервалі часу від моменту одержання особистого (секретного) ключа до моменту закінчення терміну його дії.

Очевидно [51, 96], найшвидшим (найменш складним) алгоритмом атаки типу «Повне розкриття» випадкових неслабких кривих над полями $F(p)$, $F(2^m)$ і $F(p^m)$ на сьогоднішній день є паралельний ρ-метод Полларда. Його складність оцінюється як залежність вигляду

$$\mathrm{O}(\sqrt{\pi n/4}/r) \tag{3.32}$$

від порядку базової точки n та кількості працюючих паралельно процесорів r.

Для обчислення складності вирішення дискретного логарифмічного рівняння (3.25) може бути застосована наближена формула

$$I = \sqrt{\pi n/4}/r. \tag{3.33}$$

Метод був запропонований J. Pollard для обчислення дискретного логарифма в (Z / nZ). Ідея полягає в тому, що для будь-якого кінцевого набору W

і відображення $F: W \to W$, послідовність $(w_k)_{k \in N_0}$ формується за правилом $w_0 \in W$, $w_{k+1} = F(w_k)$, де $k \in N_0$ в остаточному підсумку замкнута [51, 96]. Тобто існують цілі числа $\lambda \geq 1$ та $\mu \geq 0$ – такі, що $w_0, \ldots, w_{\mu+\lambda-1}$ є попарно визначеними та $w_k = w_{k+\lambda}, k \geq \mu$. Припускаючи, що $w_0 \in W$ вибирається випадково (тобто щодо рівномірного розподілу) і F – випадкове відображення, очікувані значення для μ і λ перебувають близько до $\sqrt{\pi |W|}/8 = 0.626...\sqrt{|W|}$. Нехай n буде порядком базової точки G, що є генератором групи $\langle G \rangle$, відкритий ключ Q буде точкою на еліптичній кривій. Для обчислення дискретного логарифма $d = \log_G Q$ Поллард використав інтерполяційну функцію $F: (Z/nZ)^* \to (Z/nZ)^*$, що має вигляд:

$$F(Y) = \begin{cases} G+Y, & \text{якщо } 1 < Yx^* \leq n/3 \\ Y+Y, & \text{якщо } n/3 < Yx^* \leq 2n/3 \\ Q+Y, & \text{якщо } 2n/3 < Yx^* < n \end{cases} \tag{3.34}$$

де Yx^* позначає x-координату точки Y, хоча це може бути так само й y-координата, визначає послідовність точок (Y_k) за правилом $Y_0 = O_E$ або $(Y_0 = G, Y_0 = Q, Y_0 = G+Q)$. Наступна точка обчислюється за формулою $Y_{k+1} = F(Y_k)$. Існують послідовності (α_k) і (β_k) – такі, що $Y_k = \alpha_k G + \beta_k Q$, отримані з правил:

$$\begin{aligned} &\alpha_0 = 0, \alpha_{k+1} \equiv \alpha_k + 1, 2\alpha_k, \text{, або } \alpha_k \bmod (n-1), k \in N_0 \\ &\beta_0 = 0, \beta_{k+1} \equiv \beta_k + 1, 2\beta_k, \text{, або } \beta_k \bmod (n-1), k \in N_0 \end{aligned} \tag{3.35}$$

завдяки трьом випадкам, описаним вище. Також існує альтернативний спосіб обчислення α_k і β_k для кожної точки Y_k – це кількість точок Q і G, які беруть участь у створенні даної точки Y_k.

Збіг пари елементів Y_i і Y_j означає, що $Y_i = Y_j$ при $i \neq j$ і дає рівняння для поля Галуа $F(p)$:

$$\alpha_j G + \beta_j Q \equiv \alpha_i G + \beta_i Q \pmod p, i \neq j. \tag{3.36}$$

Якщо розрахунок ведеться для розширеного поля $F(2^m)$ або $F(p^m)$, то рівняння береться за модулем основи поля 2 або p відповідно й понижувального полінома $f(x)$. Перетворюючи рівняння, одержимо:

$$Q = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} G \pmod p. \tag{3.37}$$

Якщо порівняти отримане рівняння з рівнянням дискретного логарифма еліптичних кривих, дістанемо, що особистий ключ можливо одержати, розв'язавши рівняння вигляду:

$$d = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} \pmod n, \beta_i \neq \beta_j. \tag{3.38}$$

Фізичний сенс полягає у прискоренні знаходження d за допомогою інтерполяційної функції $F(Y)$. За великих значень n такий алгоритм стає неефективним. Було доведено, що можливо зменшити складність, якщо всю множину точок, разом із функцією нескінченності, розбивати на $r > 3$ не пересічені множини [7, 51, 96]. У цьому випадку функція $F(Y_i)$ має вигляд:

$$Y_{i+1} = F(Y_i) = \begin{cases} (Y_i + c_1 G + d_1 Q), & \text{якщо } Y_i \in S_1; \\ (Y_i + c_2 G + d_2 Q), & \text{якщо } Y_i \in S_2; \\ \vdots & \\ (Y_i + c_r G + d_r Q), & \text{якщо } Y_i \in S_r; \end{cases} \quad (3.39)$$

де c_j, d_j – випадкові цілі числа з інтервалу $[0, n-1]$.

У [96, 115] визначено, що використання функції вигляду (3.39) дозволяє обчислення виконувати паралельно, тобто для різних областей значень процес пошуку коефіцієнтів α_k і β_k, для яких виконується умова (3.36), робити відразу на r процесах.

Якщо числа c_j, d_j вибирати таким чином, щоб не було перетинання областей Y_i у множинах, тоді можливо кожну множину додатково розбити на необхідне число підмножин. Це дозволяє завдання виконувати паралельно із задіянням необхідних r незалежних процесів. Результати роботи кожного із завдань додають у базу даних. Центральний процесор виконує паралельний пошук значень

$$Y_i = Y_j, (i \neq j). \quad (3.40)$$

На завершення за допомогою (3.38) обчислюється особистий ключ d.

3.2.3. Виведення й аналіз класичної формули визначення складності дискретного логарифмування в групах точок еліптичної кривої

Розглянемо виведення визначення очікуваної кількості елементів множини розмірності n, які повинні бути обрані випадково із заміною, перш ніж будь-який елемент буде обраний двічі. Також розглянемо випадок, коли кількість елементів, збережених і доступних для колізії, обмежена [96, 115]. По суті будемо вирішувати задачу без урахування значення колізії P_k, тобто правильного розв'язання.

Теорема 1 [96]. Нехай X – випадкова змінна для числа елементів, обраних до появи повтору. Тоді математичне сподівання

$$E(X) = \sqrt{\pi n / 2}. \quad (3.41)$$

Доказ. $\Pr(X > k) = (1-1/n)(1-n/2)...(1-(k-1)/n) \approx e^{-k^2/(2n)}$ для великих n та $k = O()\sqrt{n}$.

$$E(X) = \sum_{k=1}^{\infty} k \cdot \Pr(X = k) = \sum_{k=1}^{\infty} k \cdot (\Pr(X > k-1) - \Pr(X > k) = \sum_{k=0}^{\infty} \Pr(X > k).$$

Таким чином, очікуване число елементів, обраних до повторення:

$$E(X) \approx \sum_{k=0}^{\infty} e^{-x^2/(2n)} = \int_0^{\infty} e^{-x^2/(2n)} dx = \sqrt{\pi n / 2}. \quad (3.42)$$

Помилка в заміні (апроксимації) суми інтегралом дорівнює максимум 1, тому що функція монотонно убуває й ніколи не перевищує 1. Поданий інтеграл є стандартним.

Зрозуміло, що для формули (3.42) необхідна реалізація, яка в змозі зберігати всі обчислені значення. Тобто ресурси пам'яті для виконання атаки повинні складати приблизно $\sqrt{\pi n/2}$ елементів пам'яті, де кожний елемент пам'яті дорівнює кількості байтів, необхідних для зберігання однієї точки. Так, для зберігання однієї точки розмірністю 192 біта необхідно 24 байта, тобто для зберігання точок, необхідних для досягнення практично гарантованого успіху потрібно $24\sqrt{\pi n/2} = 1{,}875 \cdot 2^{100}$ байтів, або $1{,}875 \cdot 2^{70}$ Гбайтів дискового простору [52], що фізично неможливо при нинішньому розвитку обчислювальної техніки.

Тобто на даний момент не існує можливості виконати криптоаналіз системи з досить великим розміром параметрів з використанням методу, що зберігає всі обчислені точки. Тому оцінимо очікуване число кроків у тому випадку, коли криптоаналітик володіє певним обмеженим обсягом пам'яті.

Позначимо через z кількість елементів, які можуть бути збережені в пам'яті. Після того, як пам'ять повністю заповнена, може бути здійснена колізія тільки із z збереженими елементами. Тобто перезапис елементів у пам'яті не передбачається [96].

Теорема 2. Нехай Y буде випадковою змінною для кількості елементів, обраних перш ніж відбувся збіг, у разі якщо обсяг пам'яті дорівнює z. У такому випадку $E(Y) = \sum_{k=0}^{z-1} e^{-k^2/(2n)} + (n/z)e^{-z^2/(2n)}$.

Доказ. Ця задача аналогічна попередній за умови, що X зростає не нескінченно, а до $k = z$, після цього ймовірність здійснення колізії дорівнює z/n на кожному кроці.

$$\Pr(Y > k) \approx \begin{cases} e^{-k^2/(2n)} \\ (1 - z/n)^{k-z} e^{-z^2/(2n)} \end{cases} \quad \text{якщо} \quad (k < z), \text{ у протилежному випадку}$$

$$E(Y) = \sum_{k=0}^{z-1} e^{-k^2/(2n)} + (n/z)e^{-z^2/(2n)}.$$

Розглянуті вище варіанти припускають, що криптоаналітик може провести необмежену кількість обчислень. Тобто його обчислювальні ресурси та кількість спроб нескінченні (обмеження можуть бути накладені тільки на обсяг пам'яті).

Однак результати складності розв'язання задачі дискретного логарифма, отримані вище, на теперішній момент чисто теоретичні, оскільки не існує можливості задіяти необмежений обчислювальний ресурс для полів великої розмірності. Таким чином, актуальною стає задача визначення ймовірності, з якою дії криптоаналітика у разі злому системи досягнуть поставленої мети за обмеженого обчислювального ресурсу (обчислювальної потужності криптоаналітичної системи) чи навпаки та виведення параметризованої формули.

3.2.4. Оцінка складності криптоаналізу на основі ρ-методу Полларда з урахуванням імовірності колізії

Під час розгляду цієї моделі будемо вважати, що поява значення $\rho(Z_v)$ відбувається випадково. Будемо шукати ймовірність $P(n, k)$ того, що серед значень $\rho(Z_v)$ принаймні два співпадуть. Позначимо через $R(n, k)$ імовірність того, що при

k обчисленнях значень збігу не буде, тобто умова $\rho(Z_i) = \rho(Z_j)$ не виконується. Оскільки $P(n, k)$ і $R(n, k)$ складають повну групу подій, то

$$P(n,k)+R(n,k)=1$$

та

$$P(n,k)=1-R(n,k). \tag{3.43}$$

Визначимо $R(n, k)$. Для цього знайдемо число способів N_1 обчислення $\rho(Z_v)$, коли при k експериментах збігу не буде. При обчисленні $\rho(Z_1)$ маємо n значень без повторення, при $\rho(Z_2)$ – $(n-1)$ значень,..., при $\rho(Z_k)$ – $(n-(k-1))$ значень. Тому:

$$N_1 = n(n-1)(n-2)..(n-(k-1)).$$

Далі з незалежною появою $\rho(Z_v)$ в n обчисленнях маємо $N_з$ – число подій, причому:

$$N_з = n^k,$$

значить:

$$R(n,k)=\frac{N_1}{N_з}=\frac{n(n-1)(n-2)..(n-(k-1))}{n^k}. \tag{3.44}$$

Підставивши (3.44) у (3.43), маємо:

$$P(n,k)=1-\frac{n(n-1)(n-2)..(n-(k-1))}{n^k}. \tag{3.45}$$

Формула (3.45) точна і дозволяє обчислити ймовірність колізії за відомих n та k. Але важливим є завдання розв'язання параметричного рівняння (P,n,k), коли один або два параметри змінні. Якщо необхідно обчислити $P(n,k)$ при змінюваних (n,k), враховуючи те, що n та k, як правило, не досить великі, при обчисленнях краще використати (3.45) у вигляді [7, 96]:

$$\begin{aligned} P(n,k)&=1-\frac{n}{n}\cdot\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)..\left(\frac{n-(k-1)}{n}\right)= \\ &=1-\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)..\left(1-\frac{k-1}{n}\right) \end{aligned} \tag{3.46}$$

Але за реальних значень k при проведенні криптоаналізу, як буде показано, обчислення (3.46) потребує значних ресурсів. Окрім того, як основний предмет нас цікавить знаходження параметра k як параметра оцінки складності криптографічного аналізу методом «повного розкриття», тобто знаходження особистого ключа d_x.

У нашому випадку $k < n$, тому $x \equiv \frac{k}{n} < 1$. Для цієї умови можна скористатися тим, що:

$$(1-x)\approx e^{-x}, \tag{3.47}$$

але, звичайно, оцінюючи похибку при заданих значеннях (n,k).

Підставивши в (3.46) $\left(1-\frac{i}{n}\right)=e^{-\frac{i}{n}}$, маємо:

$$P(n,k)=1-e^{-\frac{1}{n}}\cdot e^{-\frac{2}{n}}\cdot\ldots\cdot e^{-\frac{k-1}{n}}. \tag{3.48}$$

Вирази в показниках ступеня – це члени арифметичної прогресії, перший член $\frac{1}{n}$, а число членів дорівнює $k-1$, тому [96]:

$$P(n,k)=1-e^{-\left(\frac{1}{n}+\frac{k-1}{n}\right)\frac{k-1}{2}}=1-e^{-\frac{k(k-1)}{2n}}. \qquad (3.49)$$

Таким чином, вираз (3.49) пов'язує між собою три основні параметри – імовірність колізії $P(n,k)=P_k$, складність криптоаналізу методом ρ-Полларда $k=I$ та розмір простору значення базової точки – з порядком базової точки n.

Надалі будемо подавати (3.49) у вигляді:

$$1-P_k=e^{-\frac{k(k-1)}{2n}},$$

або

$$\ln(1-P_k)=-\frac{k(k-1)}{2n}.$$

Після простих перетворень одержимо:

$$I^2-I+2n\ln(1-P_k)=0. \qquad (3.50)$$

Рівняння (3.50) неточне. Похибка пов'язана з використанням наближення $(1-x)\approx e^{-x}$ і буде оцінена нижче.

Проведемо аналіз рівняння (3.50).

1. Точне значення складності з урахуванням наближення (3.47) одержимо, вирішивши рівняння другого ступеня.

2. Враховуючи те, що $I^2 \gg I$, можна скористатися наближенням:

$$I^2 \approx -2n\ln(1-P_k)$$

або

$$I_\rho \approx \sqrt{-2n\ln(1-P_k)}. \qquad (3.51)$$

3. При $P_k = 0{,}5$ одержимо оцінку:

$$I_{0,5} \approx \sqrt{-2n\ln 2^{-1}} = \sqrt{2\ln 2n} \approx 1{,}17\sqrt{n}. \qquad (3.52)$$

4. При $P_k = 0{,}99$ одержимо оцінку:

$$I_{0,99} \approx \sqrt{-2n\ln 10^{-2}} = \sqrt{4\ln 10n} \approx 3{,}03\sqrt{n}. \qquad (3.53)$$

3.2.5. Оцінка складності криптоаналізу на основі λ-методу Полларда з урахуванням імовірності колізії

Розгляд методу λ-Полларда проведемо в такий спосіб [51, 96]. Розглядаються два процеси $\rho_1(Z_i)$ і $\rho_2(Z_j)$. Причому вважається, що колізія відбулася, якщо:

$$\rho_1(Z_i) = \rho_2(Z_j). \qquad (3.54)$$

За таких самих умов, за яких вирішувалося завдання методом ρ-Полларда, подія може здійснитися з імовірністю $P=\frac{1}{n_G}$, де n_G, як і раніше, – порядок базової точки. Далі, імовірність події, що

$$\rho_1(Z_i) \neq \rho_2(Z_j)$$

становить з першою повну групу подій, тому:

$$R(\rho_1(Z_i) \neq \rho_2(Z_j)) = 1 - \frac{1}{n_G}. \quad (3.55)$$

Якщо розглядати k таких послідовних дій, то ймовірність того, що $\rho_2(Z_1)$, $\rho_2(Z_2)$, ..., $\rho_2(Z_k)$ не будуть збігатися з $\rho_1(Z_i)$, можна обчислити як

$$R(\rho_1(Z_i) \neq \rho_2) = \left(1 - \frac{1}{n_G}\right)^k.$$

Імовірність того, що не відбулося жодного збігу для ρ_1 і ρ_2 (при всіх $Z_1, Z_2, ..., Z_k$ для ρ_1 і ρ_2):

$$R\left(\rho_1(Z_i) \underset{\forall i,j}{\neq} \rho_2(Z_j)\right) = \left(\left(1 - \frac{1}{n_G}\right)^k\right)^k = \left(1 - \frac{1}{n_G}\right)^{k^2}. \quad (3.56)$$

Далі, імовірність того, що хоча б одне значення $\rho_1(Z_i)$ збігається з $\rho_2(Z_j)$ для всіх значень k:

$$R(\rho_1(Z_i) = \rho_2(Z_j)) = 1 - \left(1 - \frac{1}{n_G}\right)^{k^2}. \quad (3.57)$$

Таким чином, співвідношення (3.57) у загальному вигляді визначає ймовірність колізії за λ-методом Полларда.

Як уже було обґрунтовано стосовно ρ-Полларда методу, рівняння (3.57) необхідно подати у вигляді, зручному для обчислень при параметрах $P_k = R(\rho_1(Z_i) = \rho_2(Z_j))$, n_G і k. Враховуючи [1–3, 5] $n_G \geq 2^{160}$, з великою точністю справедливе (3.47), тому

$$1 - \frac{1}{n_G} = e^{-\frac{1}{n_G}}. \quad (3.58)$$

Підставивши (3.58) у (3.57), маємо:

$$P_k = 1 - e^{-\frac{1}{n_G}k^2} = 1 - e^{-\frac{k^2}{n_G}}. \quad (3.59)$$

Формула (3.59) наближена, в тому розумінні, що в повну групу подій включено k^2 подій, що колізія не відбувається. А потім у (3.59), по суті, додається ще одна подія, коли відбувається колізія ($(\rho_1(Z_i) = \rho_2(Z_j))$. Таким чином, подій більше, ніж може відбутися, тобто $k^2 + 1$.

Отримаємо уточнену формулу, аналогічну (3.57). Нехай можливі $k(k-1)$ подій, коли колізія не відбувається, й одна подія, коли відбувається одна колізія. Тоді уточнена за цієї умови формула (3.59) має вигляд:

$$P(\rho_1(Z_i) = \rho_2(Z_j)) = 1 - \left(1 - \frac{1}{n_G}\right)^{(k^2-1)}. \quad (3.60)$$

Далі, з урахуванням (3.58), маємо:

$$P_k = 1 - e^{-\frac{1}{n_G}(k^2-1)} = 1 - e^{\frac{k^2-1}{n_G}}. \quad (3.61)$$

Формула (3.61) найбільш точна, тому надалі будемо розглядати саме її. Оскільки складність криптоаналізу $I = k$, то після ряду перетворень одержимо, аналогічно (3.50):

$$I^2 - 1 + n\ln(1 - P_k) = 0. \quad (3.62)$$

Порівнявши (3.62) з (3.50), бачимо, що в (3.62) замість $2n$ присутній параметр n. Розв'язання рівняння (3.62) дає точний результат відносно I. Причому негативний результат не є розв'язанням рівняння (3.62). По суті, рівняння (3.62) – це параметричне рівняння. Фіксуючи або змінюючи два параметри з трьох, можна визначити третій.

Оскільки $I^2 \gg 1$, то (3.62) можна подати у вигляді:

$$I^2 = -n\ln(1 - P_k)$$

або

$$I_\lambda = \sqrt{-n\ln(1 - P_k)}. \quad (3.63)$$

Але в кожному експерименті для λ потрібно паралельно проводити обчислення для двох процесів. Тому для загального випадку [96] замість (3.63) потрібно брати:

$$I_\lambda = 2\sqrt{-n\ln(1 - P_k)}: \quad (3.64)$$

при $P_k = 0{,}5$ маємо:

$$I_{0,5} \approx 2\sqrt{-n\ln 2^{-1}} = 1{,}68\sqrt{n};$$

при $P_k = 0{,}99$ маємо:

$$I_{0,99} \approx 2\sqrt{-n\ln 10^{-2}} = 4{,}28\sqrt{n}.$$

Точним буде рівняння:

$$I = 2\sqrt{-n\ln(1 - P_k) + 1}.$$

3.2.6. Порівняння складності криптоаналізу

Проведемо порівняння складностей методів криптоаналізу, формули для яких виведено вище [96] та проаналізуємо їх відповідність класичним формулам оцінки складності криптоаналізу криптоперетворень у групах точок еліптичних кривих. Порівняння методів проведемо з використанням (3.51) та (3.63):

$$\mu_1 = \frac{I_\rho}{I_\lambda} = \frac{\sqrt{-2n\ln(1 - P_k)}}{2\sqrt{-n\ln(1 - P_k)}} = \frac{\sqrt{2}}{2} = 0{,}707.$$

Аналогічно, при $P_k = 0{,}99$:

$$\mu_{0,99} = \frac{3{,}03\sqrt{n}}{4{,}28\sqrt{n}} = 0{,}707. \quad (3.65)$$

Таким чином, як і для класичних формул розрахунку складності, ρ-Полларда метод менш складний у порівнянні з λ-методом Полларда. Порівняємо також складність оптимального ρ-методу Полларда, розраховану за допомогою класичних формул з ρ-методом та λ-методом Полларда, використовуючи (3.33), (3.51) і (3.63):

$$\mu_2 = \frac{I_{\rho opm}}{I_\rho} = \frac{\sqrt{\pi n/4}}{\sqrt{-2n\ln(1-P_k)}} = \sqrt{\frac{\pi/4}{2\ln\left(\frac{1}{1-P_k}\right)}} = \sqrt{\frac{\pi}{8\ln\left(\frac{1}{1-P_k}\right)}},$$

$$\mu_3 = \frac{I_{\rho opm}}{I_\lambda} = \frac{\sqrt{\pi n/4}}{2\sqrt{n\ln\left(1-P_k\right)^{-1}}} = \sqrt{\frac{\pi/4}{4\ln\left(\frac{1}{1-P_k}\right)}} = \sqrt{\frac{\pi}{16\ln\left(\frac{1}{1-P_k}\right)}}. \quad (3.66)$$

Підставивши в (3.66), наприклад, $P_k = 0{,}5$, одержимо:

$$\mu_2 = \sqrt{\frac{3{,}14}{8\ln 2}} = 0{,}57,$$

$$\mu_3 = \sqrt{\frac{3{,}14}{16\ln 2}} = 0{,}285.$$

Підставивши в (3.66), наприклад, $P_k = 0{,}99$, одержимо:

$$\mu_2 = \sqrt{\frac{3{,}14}{8\ln 100}} = 0{,}09,$$

$$\mu_3 = \sqrt{\frac{3{,}14}{16\ln 2}} = 0{,}046.$$

Оскільки $\mu_2 < 1$ та $\mu_3 < 1$, то співвідношення складностей різних методів криптоаналізу зберігаються. Значне ж зростання величини складності криптоаналізу при використанні (3.51), (3.64) пояснюється тим, що формула враховує ймовірність колізії.

Оцінимо величину похибки. Необхідно виділити два джерела похибок. Перше – це перехід від $1-\frac{1}{n}$ до $e^{-1/n}$, друге – це неврахування у формулах (3.50) та (3.51) значення k.

У першому випадку абсолютну похибку за рахунок апроксимації можна визначити:

$$\delta_a = \left|1-\frac{1}{n}-e^{-1/n}\right|, \quad (3.67)$$

а відносну похибку:

$$\delta_e = \left|\frac{1-1/n-e^{-1/n}}{1-1/n}\right|. \quad (3.68)$$

Похибку щодо складності можна оцінити, використавши (3.50) та (3.51). Як результат маємо:

$$\Delta_a = \left| \frac{I^2 - I + 2n\ln(1-P_k) - I^2 - 2n\ln(1-P_k)}{I^2 - I + 2n\ln(1-P_k)} \right| = \left| \frac{-I}{I^2 - I + 2n\ln(1-P_k)} \right|. \quad (3.69)$$

Абсолютна похибка:

$$\Delta_a = \left| I^2 - I + 2n\ln(1-P_k) - I^2 - 2n\ln(1-P_k) \right| = \left| -I \right|. \quad (3.70)$$

У таблиці 3.3 [96] наведені значення складності криптоаналізу методом отримання з використанням формул (3.51), (3.64).

Таблиця 3.3. **Складність розв'язання дискретного логарифмічного рівняння в групі точок ЕК з імовірністю $P_k = 0{,}99$**

Метод	n								
	2^{128}	2^{160}	2^{192}	2^{224}	2^{256}	2^{384}	2^{512}	2^{571}	2^{1021}
ρ-метод Полларда	$3{,}03 \cdot 2^{64}$	$3{,}03 \cdot 2^{80}$	$3{,}03 \cdot 2^{96}$	$3{,}03 \cdot 2^{112}$	$3{,}03 \cdot 2^{128}$	$3{,}03 \cdot 2^{192}$	$3{,}03 \cdot 2^{256}$	$4{,}27 \cdot 2^{285}$	$4{,}27 \cdot 2^{510}$
λ-метод Полларда	$4{,}28 \cdot 2^{64}$	$4{,}28 \cdot 2^{80}$	$4{,}28 \cdot 2^{96}$	$4{,}28 \cdot 2^{112}$	$4{,}28 \cdot 2^{128}$	$4{,}28 \cdot 2^{192}$	$4{,}28 \cdot 2^{256}$	$6{,}03 \cdot 2^{285}$	$6{,}03 \cdot 2^{510}$

Наведені в таблиці 3.3 дані підтверджують висновки щодо великої складності криптоаналізу методами Полларда та неможливості їх реалізації уже при порядку базової точки $n = 2^{512}$, оскільки порядок базової точки вже наближається до числа атомів нашого всесвіту.

3.2.7. «Повне розкриття» на основі підписаних даних

Згідно сучасних понять і поглядів стійкість усіх наведених алгоритмів ЕЦП заснована на складності розв'язання дискретного логарифму в групі точок еліптичної кривої. Для знаходження секретного ключа необхідно розв'язати відносно d:

– у разі ECDSA і ECSS – рівняння

$$Q = d \times G; \quad (3.71)$$

– у разі EC-GDSA і EC-KCDSA – рівняння

$$Q = d^{-1} \times G; \quad (3.72)$$

– у разі ДСТУ 4145-2002 – рівняння

$$Q = -d \times G. \quad (3.73)$$

Розглянемо можливість знаходження d на основі атаки за відомих підписаних (перехоплених) повідомлень. Нехай перехоплено i підписаних повідомлень. Розв'язуючи для ECDSA рівняння $s = k^{-1}(dr + e) \bmod n$ відносно d, одержимо $d = {(ks - e)}/{r} \pmod n$.

Для i повідомлень одержимо i рівнянь з $i + 1$ невідомими, тобто $k_1, k_2, \ldots, k_i$ і d:

$$\begin{cases} d = {(k_1 s_1 - e_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(k_i s_i - e_i)}/{r_i} \bmod n. \end{cases} \tag{3.74}$$

$$\begin{cases} d = {(k_1 - s_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(k_i - s_i)}/{r_i} \bmod n. \end{cases} \tag{3.75}$$

Для алгоритму ДСТУ 4145-2002, використовуючи рівняння $s = (dr + k) \bmod n$, також одержуємо i рівнянь з $i+1$ невідомими:

$$\begin{cases} d = {(s_1 - k_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(s_i - k_i)}/{r_i} \bmod n. \end{cases} \tag{3.76}$$

Аналогічно, використовуючи алгоритми EC-GDSA і EC-KCDSA, можна одержати відповідно системи порівнянь порядку i з $i + 1$ невідомими.

Таким чином, для повного розкриття, тобто визначення секретного ключа d по i отриманим ЕЦП, необхідно розв'язувати систему i-го порядку з $i + 1$ невідомими.

У випадку, якщо повідомлення M є зашифрованим, то невідомими є значення геш-функцій $e_1, e_2, \ldots e_i$. Як результат одержимо систему рівнянь з $2i+1$ невідомими, тому шифрування підписаних повідомлень дозволяє істотно підвищити стійкість.

У цілому, зважаючи на наведені вище результати, можна зробити такі висновки.

1. Існує велика кількість методів криптоаналізу криптографічних перетворень у групах точок еліптичної кривої; у розділі наведено класифікацію методів криптоаналізу, їх систематизацію та огляд.

2. Відомо, що складність криптоаналізу в групі точок еліптичних кривих є експоненційно складною. У розділі розглянуто теореми та доведення формул,

що аналітично доводять складність криптоаналізу. Показується, що ці формули припускають, що криптоаналітик може провести необмежену кількість обчислень, тобто його обчислювальні ресурси та кількість спроб нескінченні (обмеження можуть бути накладені тільки на обсяг пам'яті).

Однак результати оцінки складності розв'язання задачі дискретного логарифма, отримані вище, на цей час чисто теоретичні, оскільки не існує можливості задіяти необмежений обчислювальний ресурс для полів великої розмірності. Таким чином, актуальною є задача визначення ймовірності, з якою дії криптоаналітика при зламуванні системи досягнуть поставленої мети за обмеженого обчислювального ресурсу (обчислювальної потужності криптоаналітичної системи). Чи навпаки – складності криптоаналізу системи в тих випадках, коли задана ймовірність правильного результату. У розділі наведено виведення формул, які дозволяють оцінити складність криптоаналізу криптографічних перетворень у групі точок еліптичних кривих методами ρ-Полларда та λ-Полларда у тому випадку, коли задана ймовірність, з якою необхідно досягти успіху. Доведено, що в цілому зберігаються пропорції оцінки складності для цих методів.

3.3. ОЦІНКА СТІЙКОСТІ ЕЦП ВІД АТАК ТИПУ «ЕКЗИСТЕНЦІЙНА ПІДРОБКА»

Цей вид загрози виникає за наявності слабкостей у геш-функції, яка використовується при виробленні ЕЦП. По суті, геш-функція відображає дані $m \in M$ на множину значень $h \in H$, де безліч $H \subset M$. Як наслідок можливі колізії, при яких для $h = H(m)$ знаходять $h' = H(m')$ – таке, що $h = h'$, за умови що $m \neq m'$. Для захисту від екзистенціальної підробки на геш-функцію накладається вимога, щоб складність алгоритму створення колізії мала експоненційний характер.

При доведенні стійкості ЕЦП вважається, що геш-функція є випадковою «чорною скринькою» (оракулом), на вхід якого надходять випадкові запити m_0, m_1, m_2..., а на виході формуються випадкові відповіді h_0, h_1, h_2... При поліноміальній складності всі запитання й відповіді оракул у змозі запам'ятати, і якщо на вхід надходить $m_i = m_j$ та $i \neq j$, то він видає раніше обчислену відповідь, тобто геш-значення.

На практиці геш-функція повинна задовольняти, принаймні, таким вимогам:

– не вище ніж поліноміальна складність обчислення геш-значення h;

– однонаправленість, яка полягає у неможливості обчислення даних (прообразу) m за відомим образом h (наприклад, має не нижче ніж експонентну складність);

– захищеність від знаходження для m_1 другого прообразу m_2 – такого, що $H(m_1) = H(m_2)$, складність знаходження m_2 повинна мати експоненційний характер;

– захищеність від колізій, за яких практично неможливо знайти два прообрази m_1 і m_2 – такі, що $H(m_1) = H(m_2)$, тобто складність знаходження двох прообразів m_1 і m_2 також повинна мати експоненційний характер.

Якщо геш-функція, що використовується, не забезпечує захист від колізій, то можна знайти $H(m_1) = H(m_2)$, де m_1 дійсні, заздалегідь підписані дані легальним користувачем. Потім він приєднує ЕЦП $\langle r, s \rangle$ для даних m_1 до даних m_2 та відсилає підписані дані $\langle m_2, \langle r, s \rangle \rangle$. Одержувач при перевірці ЕЦП не виявить підробки, і йому будуть нав'язані хибні дані m_2.

3.4. ОЦІНКА СТІЙКОСТІ ЕЦП ВІД АТАК ТИПУ «СЕЛЕКТИВНА ПІДРОБКА»

Сутність такої підробки полягає в тому, що при невідомому особистому ключі d для заздалегідь обраних даних (повідомлення) m необхідно сформувати такий підпис $\langle r, s \rangle$, щоб перевірка на цілісність і справжність підписаних даних m давала позитивний результат.

Розглянемо умови (алгоритм) підробки підпису для EC-DSA.

1. Формуємо чи вибираємо ключ сеансу $k_x \in \{1, 2, ..., n-1\}$.

2. Обчислимо відкритий ключ сеансу $r_x = \pi(k_x \times G)$.

3. Вибираємо чи підбираємо підпис повідомлення M_x, $s_x \in \{1, ..., n-1\}$, але за умови, що $s_x = (k_x)^{-1}(dr_x + e') \bmod n$.

4. Посилаємо чи записуємо в базу даних хибне M_x з підписом $\langle r_x, s_x \rangle$.

5. Одержувач при прийомі перевіряє цілісність і справжність повідомлення (даних) $\langle M_x, \langle r_x, s_x \rangle \rangle$. Для цього він виконує такі кроки:

1) обчислює значення геш-функції $e' = h(M_x)$;

2) обчислює значення параметрів $w = (s_x)^{-1} (\bmod n)$, $u_1 = e'w (\bmod n)$ та $u_2 = r_x w (\bmod n)$;

3) знаходить точку еліптичної кривої $(x, y) = u_1 \times G + u_2 \times Q$;

4) перетворює точку еліптичної кривої $v = \pi(x, y) \bmod n$;

5) порівнює $r_x = v$.

Перевірка на 5-му кроці буде виконана тільки в тому випадку, якщо $s_x = (k_x)^{-1}(dr_x + e') \bmod n$. Аналіз цього виразу показує, що ймовірність правильного вибору s_x у ході підробки однозначно визначається ймовірністю підбору чи угадування ключа d і складає для ЕЦП в групі точок еліптичних кривих дуже малу величину, наприклад порядку 2^{-Ld}, де Ld – довжина особистого ключа.

3.5. АНАЛІЗ ЗАХИЩЕНОСТІ ІСНУЮЧИХ ЕЦП ВІД АТАК НА ЗВ'ЯЗАНИХ КЛЮЧАХ

Особливістю цифрового підпису (ЕЦП) як криптографічного перетворення є те, що асиметрична пара ключів генерується кожним власником особисто у складі особистого та відкритого ключів. Це означає, що власник такої пари ключів може генерувати її, використовуючи спеціальні засоби, у тому числі й такі, що створюються порушником для шахрайства. Будемо вважати, що ці шахрайські дії здійснює порушник 0, 1, 2 або 3 рівнів [175]. Будемо також вважати, що ЕЦП здійснюється з використанням криптографічних перетворень у групі точок еліптичної кривої.

Як модель порушника виберемо таку, що базується на спробі селективної або екзистенційної підробки підписуваної інформації (повідомлень) [7, 64, 96]. Селективна підробка являє собою загрозу, спрямовану на створення правильного ЕЦП для попередньо обраної інформації (повідомлення) M_i. Екзистенційна підробка являє собою загрозу, яка полягає у створенні порушником правильного ЕЦП для інформації (повідомлення) M_i, можливо навіть такої, що не має сенсу. Нехай розглядається санкціонований користувач-порушник, який здійснює такі зловмисні дії. Робиться спроба для інформації (повідомлень) M_i та M_j виробити однакові ЕЦП. Далі порушник (зловмисник) може маніпулювати цими підписаними повідомленнями, пред'являючи або передаючи при реалізації загроз те чи інше повідомлення. Будемо вважати, що вибір стратегії дій зловмисником визначається прагненням одержати особисто максимальний виграш B та нанести максимальні втрати L користувачеві (власникові). Цю загрозу можна також розглядати як «атаку секретаря», коли для заздалегідь вибраних повідомлень підпис від одного M_i може бути «приклеєний» до іншого M_j.

Проведений аналіз показав [7–10, 61–73], що в цьому напрямку ведуться дослідження, є пропозиції та рекомендації. Виникає ряд проблемних питань, сутність яких у тому, що застосовувані прийняті стандарти не відповідають ряду вимог, що пред'являються до ЕЦП, перш за все стосовно стійкості проти атак на зв'язаних ключах.

Наведемо саму постановку задачі досліджень, що вирішується нижче. Розглядаються ЕЦП в групі точок ЕК, що представлені в ISO/IEC 15946-2 (ECDSA, EC-KCDSA [15, 16, 34], ГОСТ Р 34.10-2001 [47] та ДСТУ 4145-2002 [35]. Необхідно визначити захищеність цих ЕЦП від селективної підробки на основі атак зі зв'язаними ключами, наприклад k_1 та k_2. При розгляді обмежимося зв'язаними ключами (k_1, k_2); якщо відомий однин з них, інший може бути визначений не вище ніж з поліноміальною складністю. Окрім того, необхідно, якщо це можливо, визначити умови та можливості забезпечення захисту від такої загрози.

3.5.1. Аналіз захищеності ЕЦП ECDSA та EC-KCDSA

У [97] наведені результати аналізу захищеності ЕЦП ECDSA та EC-GDSA від атаки на зв'язаних ключах. Відносно ЕЦП ECDSA показано, що якщо сеансові особисті ключі k_1 та k_2 є зв'язаними, наприклад $k_1 + k_2 = n$, де n – порядок базової точки G, тоді $r_2 = r_1$ й у різних повідомлень M_i та M_j перші складові підпису r_1 та r_2 є однаковими. Далі, якщо особистий довгостроковий ключ виробити згідно з правилом

$$d_a = -\frac{h_1 + h_2}{r_1} (\mathrm{mod}\, n), \tag{3.77}$$

де h_1 та h_2 – геш-значення для повідомлень M_i та M_j, то для повідомлень M_i та M_j будуть вироблені одинакові ЕЦП, тобто $r_2 = r_1$ та $s_1 = s_2$.

Аналіз можливих наслідків відносно ЕЦП ECDSA дозволяє зробити такі висновки.

1. Загроза може бути реалізована тільки для двох наперед заданих M_i та M_j повідомлень.

2. Оскільки повідомлення M_i та M_j відомі та $r_1 = r_2$ є відкритим ключем, то й інший порушник може виробити для свого повідомлення M_v такий самий ЕЦП.

3. Із цього аналізу необхідно також зробити висновок, що при відомих h_1 та h_1, тобто повідомленнях M_i та M_j, а також завжди доступних $r_1 = r_2$ та n, порушник завжди може визначити особистий ключ. Таким чином, використання π функції вирізання тільки x координати при обчисленні відкритого сеансового параметра r ЕЦП робить стандарт ECDSA вразливим як щодо можливості створення колізій ЕЦП, так і визначення особистого ключа.

Якщо ці повідомлення обробляються в системі, то виникає загроза й для самого порушника, його особистий ключ d_a при виконанні «шахрайських» дій також компрометується. Для захисту від цієї загрози власник особистого ключа d_a повинен його змінювати відразу після появи двох таким чином підписаних повідомлень M_i та M_j.

Проведемо аналіз захищеності вдосконаленого алгоритму ЕЦП EC-KCDSA від атаки на зв'язаних ключах. Алгоритм ЕЦП EC-KCDSA визначено в [15, 16, 34]. Алгоритми вироблення та перевіряння ЕЦП EC-KCDSA наведено в таблиці 3.4.

Таблиця 3.4. **Алгоритми вироблення та перевіряння ЕЦП EC-KCDSA**

Вироблення підпису	**Перевіряння підпису**
Вхід: – особистий ключ d_a; – загальні параметри; – додаткове значення Z_a (геш-значення). Вихід: ЕЦП (r, s) для повідомлення M	Вхід: – відкритий ключ $Q_a = d_a \cdot G$, – загальні параметри, – додаткове значення Z_a (геш-значення), – підписане повідомлення M', (r', s'). Вихід: M' цілісне та справжнє або ні
1. $h = H(Z_a \parallel M)$. 2. $k \in [1, n-1]$. 3. $(x_1, y_1) = k \cdot G$. 4. Перетворення x_1 на рядок байтів c. 5. Обчислення $r = H(c)$. 6. $w = r \oplus h$, якщо $w \geq \bar{n}$, то $w = w - \bar{n}$. 7. $s = d_a(k - w) \bmod n$	1. Перевіряння, що $0 < s' < n$ та $len(r') \leq len(h())$. 2. Обчислення геш-значення $h' = H(Z_a \parallel M')$. 3. Обчислення $w' = r' \oplus h'$, якщо $w' \geq \bar{n}$, то $w' = w' - \bar{n}$. 4. Обчислення $(x_1', y_1') = s'Q_a + w'G$. 5. Перетворення x_1' на рядок байтів c. 6. Обчислення $v = H(c)$: якщо $v = r'$, то ЕЦП дійсний, інакше він відхиляється

Будемо вважати, що d_a є дійсним протягом деякого часу ΔT, а k_1 та k_2 є зв'язаними, причому $k_1 + k_2 = n$. Тоді при виробленні підпису для M_i та M_j маємо:

Для повідомлення M_i	Для повідомлення M_j
1. $h_1 = H(Z_a \parallel M_1)$ 2. $k_1 \in [1, n-1]$ 3. $(x_1, y_1) = k_1 \cdot G$ 4. $x_1 \to c_1$ 5. $r_1 = H(c_1)$ 6. $w_1 = r_1 \oplus h_1$ 7. $s_1 = d_a(k_1 - w_1) \bmod n$	1. $h_2 = H(Z_a \parallel M_2)$ 2. $k_2 = (n - k_1) \in [1, n-1]$ 3. $(x_2, y_2) = k_2 \cdot G = (n - k_1)G =$ $= nG(\bmod q) - k_1 G(\bmod q) = (x_2, y_2)$ 4. $x_2 \neq x_1 \to c_2 \neq c_1$ 5. $r_2 = H(c_2) \neq r_1 = H(c_1)$ 6. $w_2 = r_2 \oplus h_2 \neq r_1 \oplus h_2$ 7. $s_2 = d_a(k_2 - w_2) \bmod n$

Розглянемо детально та порівняємо значення на кроці 3, що отримані з використанням ключів k_1 і k_2 відповідно. Визначимо умови, за яких s компоненти ЕЦП ЕС KCDSA співпадають, тобто $s_1 = s_2$ для двох довільних різних повідомлень M_i та M_j. Використовуючи значення сьомих рядків, маємо:

$$d_a(k_1 - w_1) \bmod n = d_a(k_2 - w_2) \bmod n \tag{3.78}$$

або

$$(k_1 - w_1) \bmod n = (n - k_1 - w_2) \bmod n = -(k_1 + w_2) \bmod n \tag{3.79}$$

Далі отримаємо, що:

$$2k_1 = (w_1 - w_2) \bmod n$$

або

$$k_1 = \frac{w_1 - w_2}{2} (\bmod n) = ((r_1 \oplus h_1 - r_2 \oplus h_2) \ /2) (\bmod n) \tag{3.80}$$

Аналіз співвідношень (3.79) та (3.80) щодо захищеності EC-KCDSA дозволяє зробити такі висновки.

1. Значення відкритих ключів r_1 та r_2 відповідно для k_1 та $k_2 = n - k_1$ не співпадають, тобто в алгоритмі EC-KCDSA при цих значеннях є практично неможливою колізія r компонент ЕЦП для двох довільних повідомлень M_i та M_j. Це випливає з третього та п'ятого рядків, звідки видно, що $r_1 \neq r_2$.

2. Співвідношення (3.80) вказує на умову здійснення атаки на зв'язаних ключах. Для здійснення атаки необхідно обчислити k_1. Але k_1 залежить від r_1, яке у свою чергу однонаправлено, тобто через $H(c_1)$ залежить від k_1. Складність розв'язання рівняння (3.80) має щонайменше субекспоненційний характер. Тому здійснення атаки на зв'язаних ключах для EC-KCDSA експоненційно складне й практично неможливе.

3. Таким чином, із алгоритмів стандарту ЕЦП ISO/IEC 15946-2 ЕЦП EC-DSA є незахищеним від атаки на зв'язаних ключах, а алгоритм ЕЦП EC-KCDSA – захищеним.

3.5.2. Аналіз захищеності алгоритму ЕЦП ГОСТ Р 34.10-2001 від атаки на зв'язаних ключах

За аналогією з вищенаведеним зробимо аналіз захищеності алгоритму ЕЦП ГОСТ Р 34.10-2001 [97] від атаки на зв'язаних ключах. Алгоритм вироблення ЕЦП згідно із цим стандартом наведено в таблиці 3.5.

Таблиця 3.5. **Алгоритм ЕЦП ГОСТ Р 34.10-2001**

Вироблення підпису	**Перевіряння підпису**
Вхідні дані: – особистий ключ d, – загальні параметри ЕЦП, – повідомлення M, – модуль перетворення q. Вихідні дані: ЕЦП (r,s) для повідомлення M	Вхідні дані: – відкритий ключ Q, – загальні параметри, – ЕЦП (r',s') повідомлення M'. Вихідні дані: Повідомлення M' цілісне та справжнє або ні
1. Обчислити $h' = H(M)$ та подати у вигляді цілого числа. 2. Обчислити $h = h' (\mathrm{mod}\, q)$. 3. Генерувати випадкове k, $0 < k < q$. 4. Обчислити $R = (kG) = (x_R, y_R)$. 5. Обчислити $r = x_R (\mathrm{mod}\, q)$. 6. Обчислити $s = (rd + kh) \mathrm{mod}\, q$.	1. Перевірити, що $0 < r' < q$, $0 < s' < q$. 2. Обчислити $h_1 = H(M')$ та подати у вигляді цілого числа. 3. Обчислити $h = h_1 (\mathrm{mod}\, q)$. 4. Обчислити $v = h^{-1} (\mathrm{mod}\, q)$. 5. Обчислити значення $Z_1 = s \cdot v (\mathrm{mod}\, q)$, $Z_2 = -r \cdot v (\mathrm{mod}\, q)$. 6. Обчислити $c = (Z_1 G + Z_2 Q) \mathrm{mod}\, q = (x_c, y_c)$. 7. Визначити $R = x_c (\mathrm{mod}\, q)$. 8. Якщо $R = r'$, то підпис цілісний і справжній, інакше – ні

Виберемо, як і раніше, зв'язані ключі k_1, $k_2 = n - k_1$ та знайдемо ЕЦП для повідомлень M_i та M_j. Алгоритми вироблення ЕЦП для повідомлень M_i та M_j наведено в таблиці 3.6.

Таблиця 3.6. **Алгоритми вироблення ЕЦП зі зв'язаними ключами**

Для повідомлення M_i	**Для повідомлення M_j**
1. $h_1' = H(M_i)$. 2. $h_1 = h_1' \pmod q$. 3. $0 < k_1 < q$. 4. $R_1 = (k_1 G) = (x_{R_1}, y_{R_1})$. 5. $r_1 = x_{R_1} (\mathrm{mod}\, q)$.	1. $h_2' = H(M_j)$. 2. $h_2 = h_2' \pmod q$. 3. $k_2 = q - k_1$. 4. $R_2 = (k_2 G) = ((q - k_1)G) = -k_1 G = (x_{R_1}, -y_{R_1})$. 5. $r_2 = x_{R_1} (\mathrm{mod}\, q)$
Таким чином, незалежно від M_i та M_j завжди $r_1 = r_2 = x_{R_1} (\mathrm{mod}\, q)$	
6. $s_1 = (r_1 d + k_1 h_1) \bmod q$	6. $s_2 = (r_1 d + (q - k_1) h_2) \bmod q$

Оскільки необхідно, щоб $s_1 = s_2$, то, прирівнюючи шості рядки, маємо:

$$(r_1 d + k_1 h_1) \bmod q = (r_1 d - k_1 h_2) \bmod q,$$

звідки

$$k_1 (h_1 + h_2) = 0 (\bmod q) \tag{3.81}$$

або

$$k_1 (h_1 + h_2) = Zq. \tag{3.82}$$

Аналіз останнього порівняння показує, що існує декілька варіантів розв'язання рівняння.

По-перше. Генерується випадкове k_1 і після цього знаходиться Z – таке, що:

$$Z = \frac{k_1 (h_1 + h_2)}{q}. \tag{3.83}$$

По-друге. Обґрунтовується та формується значення Z, а після цього обчислюється:

$$k_1 = \frac{Zq}{(h_1 + h_2)}. \tag{3.84}$$

Відзначимо, що (3.83) задовольняють тільки такі значення, за яких $0 < k_1 < q$. Причому, сума $1 < h_1 + h_2 < 2q$, оскільки значення h_1 та h_2 обчислюються за модулем q. Далі $0 < k_1 < q$, тому:

$$k_1 (h_1 + h_2) < 2q^2 \quad \text{та} \quad Zq < 2q^2 \quad \text{або} \quad Z < 2q.$$

Таким чином, величина Z може приймати цілі значення з натурального ряду $1, 2, ..., 2q - 1$.

Розглянемо можливість здійснення атаки на зв'язаних ключах для алгоритму ГОСТ Р 34.10-2001, що наведений у таблиці 3.7.

Таблиця 3.7. **ЕЦП ГОСТ Р 34.10-2001**

Вироблення підпису	**Перевіряння підпису**
Вхідні дані: – особистий ключ X, – загальні параметри ЕЦП, – підписуване повідомлення M. Вихідні дані: Підписане повідомлення M з параметрами (r, s)	Вхідні дані: – відкритий ключ відправника Y, – загальні параметри, – повідомлення M' з підписом (r', s'). Вихідні дані: Повідомлення M' – цілісне та дійсне або ні
1. $h = H(M)$. 2. $0 < k < q$. 3. $R = k \cdot G$. 4. $r = \pi(R) \bmod q = X_r \bmod q$. 5. $s = (Xr + kh) \bmod q$	1. $0 < r' < q, 0 < s < q$. 2. $h_1 = H(M')$. 3. $v = (H(M'))^{q-2} \pmod q$. 4. $Z_1 = S \cdot v (\bmod q)$, $Z_2 = (q - r') \cdot v (\bmod q)$. 5. $u = Z_1 G + Z_2 Y$. 6. $U = u_X (\bmod q)$. 7. Якщо $r' = u$, то M' цілісне та дійсне

Проведемо аналіз ступеня захищеності ЕЦП від атаки на зв'язаних ключах k_1 та $k_2 = n - k_1$.

Таблиця 3.8. **Вироблення підпису на зв'язаних ключах**

Для повідомлення M_i	**Для повідомлення M_j**
1. $h_1 = H(M_i)$. 2. $0 < k_1 < q$. 3. $R_1 = k_1 \cdot G$. 4. $r_1 = \pi(R_1) = X_{k_1} \pmod q$	1. $h_2 = H(M_j)$. 2. $0 < k_2 = n - k_1 < q$. 3. $R_2 = k_2 \cdot G$. 4. $r_2 = \pi(R_2) = \pi((n-k_1)G) =$ $= \pi(nG - k_1 G) \bmod n = \pi(-k_1 G) =$ $= \pi(nG - k_1 G) \bmod n = \pi(-k_1 G) =$ $= X_{k_1} \pmod n$
Таким чином, $r_1 = r_2$	
5. $s_1 = (X \cdot r_1 + k_1 h_1) \bmod q$	5. $s_2 = (X \cdot r_1 + k_1 h_2) \bmod n$

Тепер визначимо умову, за якої $s_1 = s_2$.

$$Xr_1 + k_1 h_1 = Xr_1 + (q - k_1) h_2 \pmod q;$$

$$Xr_1 + k_1 h_1 = Xr_1 - k_1 h_2 \pmod q;$$

$$k_1 (h_1 + h_2) = 0 \bmod q.$$

Таким чином,

$$k_1 (h_1 + h_2) = Zq,$$

звідки

$$k_1 = \frac{Zq}{h_1 + h_2} \tag{3.85}$$

або

$$Z = \frac{k_1 (h_1 + h_2)}{q}. \tag{3.86}$$

Існування розв'язку рівняння та його множину оцінимо, використовуючи (3.85) і (3.86). Оскільки $1 < h_1 + h_2 < 2q$ та $0 < k_1 < q$, то

$$k_1 (h_1 + h_2) < 2q^2$$

або

$$Zq < 2q^2 \text{ та } Z < 2q.$$

У той же час цілі значення k_1 можна отримати не при всіх значеннях Z, а тільки при тих, які дають цілі значення k_1.

Таким чином, за своїми властивостями розроблений у 1999 році в Україні проект стандарту ЕЦП має властивості, ідентичні ГОСТ Р 34.10-2001 [47]. На наш погляд, ці властивості необхідно в подальшому дослідити ширше.

3.5.3. Аналіз захищеності алгоритму ЕЦП ДСТУ 4145-2002 від атаки на зв'язаних ключах

Проведемо аналіз захищеності алгоритму ЕЦП ДСТУ 4145-2002 від атаки на зв'язаних ключах k_1 та $k_2 = n - k_1$. Алгоритм вироблення ЕЦП згідно ДСТУ 4145-2002 наведено в таблиці 3.9.

Таблиця 3.9. **ЕЦП ДСТУ 4145-2002**

Вироблення підпису	**Перевіряння підпису**
Вхідні дані: – особистий ключ d, – загальні параметри ЕЦП. Вихідні дані: Підписане повідомлення (iH, M, $Д$), де i – ідентифікатор функції гешування, M – підписуване повідомлення, $Д$ – ЕЦП у вигляді (r,s) складових	Вхідні дані: – відкритий ключ Q, – загальні параметри ЕЦП, (iH, M', $Д'$), де i – ідентифікатор функції гешування, M' – одержане повідомлення, $Д = \{r', s'\}$ – ЕЦП. Вихідні дані: Підпис дійсний чи недійсний
1. Обчислити $k \in [1, n-1]$. 2. Обчислити $R = k \cdot G = (x_R, y_R)$. 3. Присвоїти $f_k = \pi(x_R, y_R) = x_R$. 4. Цифровий передпідпис (k, f_k). 5. Обчислити $h = H(M)$ та перетворити на елемент основного поля. Якщо $h = 0$, то $h = 1$. 6. Обчислити елемент основного поля $y = hf_k$ та перетворити на r. 7. Обчислити $S = (k + d \cdot r) \bmod n$. 8. Результат $(iH, M, Д = (r, S))$	1. $h = \mathrm{H}(M')$. 2. Перевірити, що $0 < r' < n$, $0 < s' < n$. 3. Обчислити $R = s'G + r'Q = (x_R, y_R)$. 4. Обчислити $y = \bar{h} \cdot x_R$ та перетворити на $\bar{r}$. 5. Якщо $r' = \bar{r}$, то підпис дійсний, інакше – недійсний

Розглянемо можливості створення колізій підписів для M_i та M_j на зв'язаних ключах k_1 та $k_2 = n - k_1$.

Для повідомлення M_i	**Для повідомлення M_j**
1. $k_1 \in [1, n-1]$. 2. $f_{k_1} = \pi(k_1 G) = \pi(x_{R_1}, y_{R_1}) = x_{R_1}$. 3. Формується передпідпис $(k_1, f_{k_1}) = (k_1, x_{R_1})$. 4. Обчислити $h_1 = H(M_i)$. 5. Обчислити елемент основного поля $y_1 = h_1 x_{R_1} = r_1$. 6. Обчислити $s_1 = (k_1 + dr_1) \bmod n$.	1. $k_2 = (n - k_1) \in [1, n-1]$. 2. $f_{k_1} = \pi((n-k_1)G = \pi(nG - k_1 G) = \pi(x_{R_1} - y_{R_1}) = x_{R_1}$. 3. Формується передпідпис $(k_2, f_{k_2}) = (k_2, x_{R_1})$. 4. Обчислити $h_2 = H(M_j)$. 5. Обчислити елемент основного поля $y_2 = h_2 x_{R_1} = r_2$. 6. Обчислити $s_2 = (k_2 + dr_2) \bmod n$.

Проведемо аналіз результатів, одержаних у 5 рядку. У цьому випадку $r_1 \neq r_2$, але r_1 та h_1 відомі, тому:

$$x_{R_1} = \frac{y_1}{h_1}; \tag{3.87}$$

$$y_2 = r_2 = h_2 \frac{y_1}{h_1} = y_1 \frac{h_2}{h_1} = r_1 \frac{h_2}{h_1}. \tag{3.88}$$

Це означає, що, знаючи r_1 та h_1, можна знайти x_{R_1}.

Таким чином, хоч $r_1 \neq r_2$, але компоненти r_1, r_2 зв'язані між собою й обчислювально легко знаходяться при відомих M_i та M_j. У подальшому необхідно детально проаналізувати цю слабкість.

Далі розглянемо умови, за яких $S_1 = S_2$.

Як результат маємо:

$$(k_1 + dr_1) \bmod n = (k_2 + dr_2) \bmod n$$

або

$$k_1 + dr_1 = \left(n - k_1 + dr_1 \frac{h_2}{h_1}\right) (\bmod n);$$

$$k_1 = 0.5\left(-dr_1 + dr_1 \frac{h_2}{h_1}\right) \bmod n = \frac{dr_1}{2}\left(-1 + \frac{h_2}{h_1}\right) \bmod n, \tag{3.89}$$

або

$$d = \frac{2k_1}{r_1\left(-1 + {}^{h_2}/_{h_1}\right)} \bmod n = \frac{2k_1 h_1}{r_1(-h_1 + h_2)} \bmod n. \tag{3.90}$$

Проведемо також аналіз рівня захищеності для випадку, коли значення y_1 та y_2 пункту 5 обчислюються у вигляді сум $y_1 = (h_1 + x_{R_1})$ та $y_2 = (h_2 + x_{R_2})$. Справа в тому, що алгоритм ДСТУ 4245-2002 є модифікацією відомого алгоритму ECSS [27, 29]. За аналогією з ДСТУ 4145-2002 маємо:

$$r_1 = y_1 = (h_1 + x_{R_1}) \tag{3.91}$$

та

$$r_2 = y_2 = (h_2 + x_{R_2}). \tag{3.92}$$

Окрім того,

$$r_2 = (h_2 - h_1 + h_1 + x_{R_1}) = (h_2 + x_{R_1}),$$

тобто r_2 зв'язане з r_1 через x_{R_1}.

Таким чином, у випадку обчислення r_1 та r_2 через суму h_1 та x_{R_1} і h_2 та x_{R_1}:

$$r_1 = (h_1 + x_{R_1}(\mathrm{k}_1)), \tag{3.93}$$

а

$$r_2 = (h_2 + x_{R_1}(\mathrm{k}_1)) = ((h_2 - h_1) + r_1). \tag{3.94}$$

При обчисленні r_1 та r_2 через добуток (рядок 5) рівняння

$$2k_1 + d(r_1 - r_2) = 0 (\bmod n)$$

при $r_1 = h_1 x_{R_1}$, $r_2 = h_2 x_{R_1}$ має вигляд:

$$(2k_1 + d(h_1 x_{R_1} - h_2 x_{R_1})) \bmod n = 0$$

або

$$2k_1 + dx_{R_1}(h_1 - h_2) \bmod n = 0. \tag{3.95}$$

Залежно від потреби розв'язання рівняння (3.95) дозволяє визначити або k_1, або d відповідно:

$$k_1 = \frac{dx_{R_1}(h_1 - h_2)}{2} (\mathrm{mod}\, n), \tag{3.96}$$

$$d = \frac{2k_1}{x_{R_1}(h_2 - h_1)} (\mathrm{mod}\, n). \tag{3.97}$$

Окрім того, при $r_2 = r_1 \frac{h_2}{h_1}$ та $r_1 = h_1 x_{R_1}$ маємо рівняння:

$$2k_1 + d\left(r_1 \frac{h_2}{h_1} - r_1\right) \mathrm{mod}\, n = 0,$$

або в остаточному вигляді:

$$2k_1 + dr_1\left(\frac{h_2 - h_1}{h_1}\right) \mathrm{mod}\, n = 0. \tag{3.98}$$

Рівняння (3.98), за необхідністю, розв'язуємо відносно невідомого або k_1, або d:

$$k_1 = \frac{dr_1(h_1 - h_2)}{2h_1}, \tag{3.99}$$

$$d = \frac{2k_1 h_1}{r_1(h_1 - h_2)}. \tag{3.100}$$

У цьому випадку, якщо $h_1 \neq h_2$, то $r_1 \neq r_2$, але r_1 та h_1 відомі, тому

$$x_{R_1} = (y_1 - h_1) = (r_1 - h_1),$$

і далі

$$r_2 = (h_2 + r_1 - h_1) = ((h_1 - h_2) + r_1).$$

Тобто r_2 також одночасно зв'язане з r_1 та h_1 і h_2. Із одержаних виразів випливає, що, знаючи r_1 та h_1, можна однозначно визначити x_{R_1}.

Наведені вище результати досліджень дозволяють зробити висновки про те, що ЕЦП за алгоритмами ДСТУ 4145-2002, а також ECSS [97] має недостатній рівень захисту від атак на зв'язаних ключах. На наш погляд, для доведення рівня його захищеності необхідно провести додаткові дослідження.

При проведенні досліджень особливу увагу необхідно звернути на те, що компоненти S_1 і S_2 співпадають, а також той факт, що r_1 та r_2 є взаємозв'язаними.

3.5.4. Загальні оцінки захищеності ЕЦП від атак на зв'язаних ключах

Проведені дослідження дозволили оцінити захищеність від атак на ЕЦП на зв'язаних ключах. Загрози такого виду можуть бути реалізовані тільки для двох наперед заданих повідомлень. Із аналізу (1) необхідно також зробити висновок, що для ECDSA при відомих h_1 та h_2, тобто повідомленнях M_i та M_j, а також завжди доступних $r_1 = r_2$ та n, порушник завжди може визначити особистий ключ. Таким чином, використання π функції вирізання тільки x координати при обчисленні відкритого сеансового параметра r ЕЦП робить стандарт ECDSA вразливим як щодо можливості створення колізій ЕЦП, так і можливості визначення особистого ключа, якщо відомі повідомлення M_i та M_j.

Якщо ці повідомлення обробляються в системі, то виникає загроза і для самого порушника, його особистий ключ d при виконанні шахрайства також компрометується. Для захисту від цієї загрози власник особистого ключа d повинен його змінювати відразу після появи двох таким чином підписаних повідомлень M_i та M_j.

Отримані результати щодо захищеності EC-KCDSA дозволяють зробити такі висновки.

1. Значення відкритих ключів r_1 та r_2 відповідно для k_1 та $k_2 = n - k_1$ не співпадають, тобто в алгоритмі EC-KCDSA за цих значень практично не можлива колізія r компонентів ЕЦП для двох довільних повідомлень M_i та M_j.

2. Для здійснення атаки необхідно обчислити k_1. Але k_1 залежить від r_1, яке у свою чергу складне, однонаправлене, через $H(c_1)$ залежить від k_1.

3. Розв'язання рівняння (4) має субекспоненційну складність. Тому здійснення атаки на зв'язаних ключах для EC-KCDSA експоненційно складне й практично не можливе.

4. Таким чином, із алгоритмів стандарту ISO/IEC 15946-2 алгоритм ЕЦП ECDSA є незахищеним від атаки на зв'язаних ключах, а алгоритм EC-KCDSA – захищеним.

Відносно ЕЦП згідно алгоритмів ДСТУ 4145-2002 а також ECSS можна зробити висновок що вони мають слабкий захист від атак на зв'язаних ключах. На наш погляд, для визначення рівня захищеності ДСТУ 4145-2002 необхідно провести додаткові дослідження. При проведенні досліджень особливу увагу необхідно звернути на те, що компоненти S_1 та S_2 співпадають, а також той факт, що r_1 та r_2 взаємозв'язані.

3.6. АНАЛІЗ ЗАХИЩЕНОСТІ ІСНУЮЧИХ ЕЦП ВІД АТАК НА ПРОГРАМНУ РЕАЛІЗАЦІЮ

Відомо, що на сьогодні тією чи іншою мірою в операційних системах знайшли розповсюдження та широко застосовуються програмні засоби реалізації електронних цифрових підписів (ЕЦП) [57–62, 126]. Окрім того, сьогодні ЕЦП широко застосувуються в різноманітних інформаційно-телекомунікаційних системах і технологіях. При цьому, хоч самі алгоритми ЕЦП відносно їх стійкості до атаки типу «Повне розкриття» достатньо добре досліджені [7–10, 96, 115], на наш погляд, залишаються відкритими питання захищеності засобів ЕЦП від атак на вид їх реалізації – програмної, програмно-апаратної та апаратної. Це стало дуже важливим також у зв'язку з широким й інтенсивним впровадженням ЕЦП в системи електронного документообігу та створенням інформаційних структур відкритих ключів, у яких також використовуються засоби ЕЦП [1–3, 6, 57–62, 101–108, 128–131]. Метою подальшого розгляду є дослідження захищеності та визначення умов і можливостей застосування програмних засобів ЕЦП, визнаних у світі та в Україні стандартів ЕЦП.

Будемо вважати, що порушником може бути розробник програмного забезпечення, користувачі та криптоаналітик. Нехай розробник програмних засобів може закласти лазівку в програмну реалізацію вироблення підпису, що може

бути керованою з його боку. Для цього він, наприклад, у програмну реалізацію або безпосередньо в операційну систему може записати «троянського коня», вірусну програму чи зробить закладку, яка у відповідний час або на відповідному етапі функціонування активізується та сформує або використає для двох різних повідомлень один і той самий ключ сеансу k. Указані дії можуть здійснювати за необхідністю також і самі користувачі. Нижче наведено результати досліджень щодо захищеності систем ЕЦП від атак на програмну реалізацію для стандартів ЕЦП, які визнані на світовому рівні – ECDSA, EC-GDSA, EC-KCDSA і включені до ISO/IEC 15946-2 [15, 16, 34], Федерального стандарту РФ ГОСТ Р 34.10-2001 [47] та національного стандарту України ДСТУ 4145-2002 [35], а також наведено рекомендації з перекриття указаних загроз.

3.6.1. Захищеність ЕЦП ISO/IEC 15946-2 від атак на реалізацію

Розглянемо можливості та умови здійснення атаки на програмну реалізацію ЕЦП, що визначені в ISO/IEC 15946-2. В алгоритмі ECDSA вироблення ЕЦП для деякого повідомлення здійснюється згідно такого алгоритму [15, 16, 34, 98]:

1. Обчислити значення функції гешування від повідомлення M $h = H(M)$.
2. Сформувати або обчислити особистий ключ сеансу $k \in [1, n-1]$.
3. Обчислити значення точки $(x_1, y_1) = k \cdot G$.
4. Обчислити відкритий ключ сеансу $r = \pi(x_1, y_1) = x_1 (\mathrm{mod}\, n)$.
5. Обчислити значення k^{-1} у полі $F(n)$.
6. Обчислити ЕЦП $s = (d_a r + h) k^{-1} \bmod n$.

Далі вважатимемо, що в деякі моменти часу через зловмисні дії при виробленні підпису два рази використовується один і той самий ключ сеансу k, тобто $k_i = k_j$ для підпису повідомлень M_i та M_j.

Далі r складові, тобто сеансові відкриті ключі:

$$r_1 = \pi(x_1, y_1) = x_1 (\mathrm{mod}\, n), \tag{3.101}$$

$$r_2 = \pi(x_1, y_1) = x_1 (\mathrm{mod}\, n). \tag{3.102}$$

Таким чином, $r_1 = r_2 = x_1 (\mathrm{mod}\ n)$.

У подальшому для S_1 та S_2 маємо:

$$S_1 = (dr_1 + h_1) k_1^{-1} (\mathrm{mod}\ n), \tag{3.103}$$

$$S_2 = (dr_2 + h_2) k_1^{-1} (\mathrm{mod}\ n). \tag{3.104}$$

Оскільки $k_1 = k_2 = k$ та $r_1 = r_2 = r = x_1 (\mathrm{mod}\ n)$, то

$$S_1 = (dr + h_1) k_1^{-1} (\mathrm{mod}\ n), \tag{3.105}$$

$$S_2 = (dr + h_2) k_1^{-1} (\mathrm{mod}\ n). \tag{3.106}$$

Розв'язавши систему рівнянь відносно d та k, отримаємо:

$$d = \frac{s_1 h_2 - s_2 h_1}{r(s_2 - s_1)} \bmod n, \tag{3.107}$$

$$k = \frac{dr + h_1}{S_1} \bmod n. \tag{3.108}$$

Таким чином, криптоаналітик (порушник) отримавши два підписані повідомлення (документи) $(M_i r_i s_i), (M_j r_j s_j)$, може визначити особистий (таємний) довгостроковий ключ d і в подальшому використовувати його для підробки підписів під фальшивими документами тощо, тобто особистий ключ буде компрометований.

За аналогією для EC-GDSA маємо [15, 34, 98]. Оскільки в результаті атаки порушнику стане відомо, що

$$k_1 = k_2 = k \in (1, n-1);$$

$$r_1 = r_2 = x_1 \pmod n = r,$$

то в подальшому, перехопивши S_1 та S_2:

$$S_1 = (k_1 r_1 - h_1) d \pmod n = (kr - h_1) d \pmod n, \tag{3.109}$$

$$S_2 = (k_2 r_2 - h_2) d \pmod n = (kr - h_2) d \pmod n, \tag{3.110}$$

та розв'язавши систему рівнянь (3.109), (3.110) відносно d, а за необхідністю й відносно k, він визначить, що:

$$d = \frac{s_1}{kr - h_1} \pmod n, \tag{3.111}$$

$$k = \frac{h_1 s_2 - h_2 s_1}{r(s_2 - s_1)} \bmod n. \tag{3.112}$$

Таким чином, і для алгоритму EC-GDSA існує ефективна атака на програмну реалізацію ЕЦП, у результаті здійснення якої компрометується довгостроковий особистий ключ цифрового підпису.

За аналогією для EC-KCDSA можна отримати [15, 34, 98]:

$$k_1 = k_2 = k \in (1, n-1);$$

$$r_1 = r_2 = r = H(c) = r;$$

$$w_1 = r_{1+} h_1 = r + h_1;$$

$$w_2 = r_2 + h_2 = r + h_2.$$

У подальшому, перехопивши підписи S_1та S_2 відповідних повідомлень:

$$S_1 = d(k - w_1) \pmod n, \tag{3.113}$$

$$S_2 = d(k - w_2) \pmod n, \tag{3.114}$$

та розв'язавши систему рівнянь (3.113) і (3.114) відносно d, а за необхідності й відносно k, отримуємо:

$$d = \frac{s_1}{(k - w_1)} \pmod n, \tag{3.115}$$

$$k = \frac{w_1 s_2 - s_1 w_2}{s_2 - s} \pmod n. \tag{3.116}$$

Наведені вище результати свідчать про те, що на всі алгоритми ЕЦП, які визначає стандарт ISO/IEC 15946-2, тобто ECDSA, EC-GDSA та EC-KCDSA, існує атака на програмну або інші реалізації, якщо тільки порушник у змозі примусити застосувати два рази один і той самий особистий (таємний) ключ сеансу, тобто $k_1 = k_2 = k \in (1, n-1)$.

3.6.2. Захищеність ЕЦП ДСТУ 4145-2002 від атак на реалізацію

Орієнтуючись на підхід та результати, отримані вище, розглянемо також умови здійснення атаки на реалізації ЕЦП ДСТУ 4145-2002 [35, 98] та EC SS [27, 98]. Як і раніше, будемо вважати, що порушник у змозі примусити засіб ЕЦП виробити $k_1 = k_2 = k \in (1, n-1)$. Тоді

$$R_1 = R_2 = kG = (x_R, y_R) = R;$$
$$fk_1 = fk_2 = x_R = fk;$$
$$y_1 = h_1 fk$$
$$y_2 = h_2 fk;$$
$$y_1 \Rightarrow r_1 ; y_2 \Rightarrow r_2;$$
$$S_1 = (k + dr_1) \pmod n \tag{3.117}$$
$$S_2 = (k + dr_2) \pmod n ; \tag{3.118}$$

Розв'язавши систему рівнянь (3.117) та (3.118) відносно d та, за необхідності, й відносно k, отримуємо:

$$d = \frac{s_1 - s_2}{r_1 - r_2} (\mathrm{mod}\, n), \tag{3.119}$$

$$k = s_1 - dr_1 (\mathrm{mod}\, n). \tag{3.120}$$

За аналогією, для алгоритму ECSS також маємо:

$$k_1 = k_2 = k \in (1, n-1);$$
$$R_1 = R_2 = kG = (x_R, y_R) = R;$$
$$fk_1 = fk_2 = fk = x_R ; +$$
$$y_1 = h_1 + fk$$
$$y_2 = h_2 + fk;$$
$$y_1 \Rightarrow r_1$$
$$y_2 \Rightarrow r_2;$$
$$S_1 = (k - dr_1) \pmod n \tag{3.121}$$
$$S_2 = (k - dr_2) \pmod n. \tag{3.122}$$

Знову розв'язуючи систему (3.121) і (3.122) відносно d та k, отримуємо:

$$d = \frac{s_1 - s_2}{r_2 - r_1} (\mathrm{mod}\, n) \tag{3.123}$$

$$k = (s_1 + d \cdot r_1) \bmod n . \tag{3.124}$$

Наведені вище результати свідчать про те, що на всі алгоритми ЕЦП, визначені стандартом ISO/IEC 15946-2, тобто ECDSA, EC-GDSA та EC-KCDSA, існує атака на програмну чи інші реалізації, якщо тільки порушник у змозі примусити застосувати два рази один і той самий особистий (таємний) ключ сеансу, тобто $k_1 = k_2 = k \in (1, n-1)$.

3.6.3. Захищеність ЕЦП ГОСТ Р 34.10-2001 від атак на реалізацію

Використовуючи підхід, що застосований вище, і для ЕЦП, визначеного ГОСТ Р 34.10-2001 [47, 98], за аналогією отримуємо:

$$k_1 = k_2 = k \in (1, n-1);$$
$$r_1 = r_2 = r;$$
$$S_1 = (rd + kh_1) \bmod n, \tag{3.125}$$
$$S_2 = (rd + kh_2) \bmod n. \tag{3.126}$$

Знову розв'язуючи систему (3.125) і (3.126) відносно d та k, отримуємо:

$$d = \frac{s_1 h_2 - s_2 h_1}{r(h_2 - h_1)} (\bmod n), \tag{3.127}$$
$$k = \frac{S_1 - rd}{h_1} (\bmod n). \tag{3.128}$$

Тобто й відносно ЕЦП ГОСТ Р 34.10-2001 [47, 98] є атаки на програмну реалізацію ЕЦП або іншу реалізацію, коли порушник у змозі примусити засіб два рази сформувати одне й те саме значення k для двох повідомлень. У результаті такої атаки порушник може визначити довгостроковий особистий d і відповідно зможе нав'язувати як хибні повідомлення, так і викривляти істинні.

У цілому, можна зробити висновок, що в Україні набули розповсюдження програмні реалізації ЕЦП [6, 98]. На наш погляд, необхідно розглянути різні можливі атаки на такі реалізації, у тому числі з боку як розробника, так і клієнта, що їх використовує. Сутність цієї задачі в такому. Нехай розробник може закласти лазівку в програмну реалізацію вироблення підпису. Для цього він, наприклад, у програмну реалізацію записує «троянського коня» або вірус, який активізується за командою і сформує або використає для двох різних повідомлень один і той самий ключ сеансу k. Можливий й інший вплив.

Таким чином, для алгоритмів ЕЦП ECDSA, EC-GDSA, EC-KCDSA, ДСТУ 4145-2002, ECSS та ГОСТ Р 34.10-2001 існують атаки на програмну реалізацію ЕЦП. Якщо порушнику вдасться змусити програму «вироблення підпису» і 2 рази використати одне й те саме значення k для двох повідомлень, то він в реальному часі визначить особистий довгостроковий ключ d і зможе нав'язувати як хибні повідомлення, так і викривляти істинні. Для захисту від такої атаки необхідно використовувати надійні засоби КЗІ типу ЕЦП у сенсі наявності на них сертифікатів відповідності, експертних висновків та обов'язкового безперервного контролю цілісності й справжності програми вироблення ЕЦП. Найкращим способом захисту від такої загрози є апаратна реалізація процедур вироблення та перевіряння ЕЦП.

3.7. АТАКИ НА ЕЦП СПЕЦІАЛЬНОГО ВИДУ ТА ЗАХИСТ ВІД НИХ

Встановлено, що гарантований захист особистих і таємних ключів від їх розголошення (компрометації) може бути забезпечено за умови апаратної або апаратно-програмної реалізації відповідних засобів КЗІ [121–123]. Указане визначає необхідність реалізації засобів КЗІ перш за все у такому вигляді. Окрім того, при апаратній

реалізації досягаються більш високі швидкості прямих і зворотних криптографічних перетворень. Але за такої реалізації засобів КЗІ потенційно можуть бути реалізованими специфічні атаки, перш за все «фізичні атаки», атаки на «криптопристрої», атаки на «реалізацію», атаки «спеціальних впливів» [127] тощо. Атаки на «криптопристрої» та на реалізацію можуть бути здійснені через застосування атак «апаратних помилок», «час виконання операцій», «енергоспоживання» тощо.

Основною метою фізичної атаки є дослідження особливостей реалізації пристрою КЗІ (мікросхеми) для отримання інформації відносно особистого або таємного ключів, наприклад шляхом дослідження області всередині кристалу ПЛІС. Тобто такі атаки орієнтовані на специфічні області ПЛІС, які в режимі нормального функціонування є недоступними.

3.7.1. Атака на основі апаратних помилок

Атака апаратних помилок полягає в тому, що порушник, маючи доступ до засобів КЗІ, або в цілому до апаратури КЗІ, має змогу проводити штатні операції в частині криптографічних перетворень вхідних даних, а також спеціальним чином впливати на процес обробки інформації з метою спричинити некоректну роботу засобів КЗІ.

Розглянемо три типи можливих атак, що ґрунтуються на створенні апаратних помилок для випадку криптографічних перетворень у групі точок ЕК. Будемо також вважати, що загальносистемні параметри та відкритий ключ відомі, а особистий (таємний) ключ записаний в електронному ключі (у тому числі старт-карті) і є недоступним у процесі його застосування. Тобто ми виключаємо із розгляду етап інсталяції електронного ключа та запису особистого ключа. Будемо також вважати, що користувач може подавати на вхід деяку точку G або послідовність точок та обчислювати відкритий ключ, наприклад, у вигляді:

$$Q = dG \pmod q.$$

Зрозуміло, що порушник не знає особистого ключа і ставить задачу його визначення в першу чергу.

Спочатку [127] будемо розглядати найпростіший варіант, коли порушник здатний здійснити збій роботи регістру протягом виконання алгоритму в строго визначеному інтервалі бітів одного з множників. Нехай також він у змозі подавати на вхід схеми обчислення відкритого ключа точки G^*, що не належать цій ЕК E, а належать іншій ЕК E^*. Причому E^* відрізняється від ЕК, що використовується коефіцієнтом b^*. У цьому випадку

$$E - E^* = (X^3 + aX + b) - (X^3 + aX + b^*) = b - b^*. \qquad (3.129)$$

Також для проведення успішного криптоаналізу порядок ЕК E^* повинен мати найменший дільник r^* – такий, що порядок точки G^*

$$ord\, G^* = r^*. \qquad (3.130)$$

Це дозволить зменшити складність розв'язання дискретного логарифму від рівня порядку r до рівня r^*, оскільки результат скалярного множення буде лежати на тій самій ЕК E^*. У цілому, така атака може бути виконана в такій послідовності:

1) генерується точка G^* на спеціальній криптографічно слабкій ЕК E^*;

2) з використанням засобу КЗІ обчислюється $d\,G^*$;

3) розв'язується задача факторизації отриманого результату $d\,G^*$ на кривій E^* за умови, що відомі r^* та G^*;

4) обчислюється $d^* = d \pmod{r^*}$;

5) повторення пунктів 1–4 для декількох різних точок G^*;

6) з використанням китайської теореми про лишки та обчислених значень d_i^* визначається особистий ключ.

Необхідно відзначити ту особливість цієї атаки, що вона може бути застосована щодо засобів КЗІ як програмних, так і апаратних. Для захисту від указаної атаки в стандартах [15, 16, 30–32, 34] вказується на необхідність перевірки базової точки G – чи належить вона еліптичній кривій E.

За вказаних умов може бути застосована інша атака внесення помилок у строго визначений період обчислень.

3.7.2. Атака на основі внесення помилок у строго визначений період обчислень

Будемо вважати, що порушник здатний реалізовувати однобітовий збій в засобі КЗІ в строго визначені моменти часу, а саме відразу після закінчення перевірки на вході та до початку виконання скалярного множення. Особливість умов цієї атаки полягає в тому, що порушник не знає реального значення G^*, що отримане під час збою.

Для заданих умов атака може виконуватися в такій послідовності.

1. Здійснюється однобітовий збій у засобі відразу ж після перевірки базової точки.

2. Обчислюється значення відкритого ключа $d\,G^*$.

3. Визначається ЕК E^*, на якій лежить точка еліптичної кривої $d\,G^*$.

4. Визначаються всі можливі значення точок G^*, а їх буде логафирм двійковий від G, а потім виконується:

а) факторизація отриманого значення точки $d\,G^*$ на кривій E^* для відомих r^* та G^*;

б) обчислюється значення $d^* = d \pmod{r^*}$.

5. Пункти 1–4 повторюються для декількох різних точок G_i^*.

6. Далі, на основі отриманих значень d_i^* та використовуючи китайську теорему про лишки, визначається дійсне значеня d.

Якщо застосовується схема направленого шифрування Ель-Гамаля, то на виході може бути виведене лише значення X – координати результату скалярного множення. У цьому випадку процедура визначення криптографічно нестійкої ЕК E^*, на якій лежить точка результату обчислення скалярного множення, значно ускладнюється. За таких умов, як правило, переходять до застосування ймовірнісної моделі [127].

3.7.3. Атака на основі внесення помилок у довільний момент обчислень

Будемо розглядати алгоритм множення точки на ЕК «справа наліво». Представимо особистий ключ у двійкому вигляді:

$$d = (d_{n-1}, d_{n-2}, \ldots d_1, d_0),$$

де d_0 – найменш значущий біт.

Для вказаної умови алгоритм множення на ЕК «справа наліво» можна записати таким чином [127].

INPUT: P, $d = (d_{n-1}, d_{n-2}, \ldots d_1, d_0)_2$

OUTPUT: $Q = dP$

1. $H = P$; $Q = 0$;
2. *for* $i = 0\, n-1$ *do*
3. *if* $(d_i = 1)$ *then* $Q = Q + H$;
4. H = 2 H;
5. Return Q.

Будемо вважати, що криптоаналітику відома довжина n особистого ключа d. Значення змінних Q, H позначимо перед i-ітерацією як $Q^{(i)}$ та $H^{(i)}$.

Атаку будемо здійснювати таким чином. Спочатку на вхід засобу КЗІ подається значення точки ЕК, що належить ЕК – E^*, після чого виконується операція скалярного множення, результатом якого є відкритий ключ

$$Q(n) = dG \pmod q,$$

який зберігається та доступний на виході засобу КЗІ. Далі виконуємо ту саму операцію скалярного множення з обчислення відкритого ключа, але за умови, що в процесі обчислення вноситься помилка у випадковий біт результату. Обчислений відкритий ключ у цьому випадку буде помилковим, позначимо його як $Q^{(n)*}$. Будемо вважати, що збій відбувся протягом j-ітерації так, що

$$n - m \le j < n.$$

А також будемо вважати, що в результаті збою інвертується один біт в регістрі збереження відкритого ключа Q. Тоді $Q^{(n)*}$ позначає результат обчислення відкритого ключа зі збоєм, який відрізняється від дійсного $Q^{(j)}$.

У подальшому необхідно знайти номер ітерації j^*, але такої, що $j^* > j$ та $d_j^* = 1$ для отриманих значень $Q^{(n)}$ та $Q^{(n)*}$. Для спрощення приймемо, що серед m найбільш значущих бітів таємного множника наявний щонайменше один ненульовий біт, тобто існує j^*. За таких умов можна знайти кандидатів на значення $Q^{(j^*)*}$ шляхом послідовного аналізу кожного номеру ітерації i в діапазоні $n - m \le j < n$ та перевірки одночасно таких умов:

1) i як кандидатуру на j^*, тобто $i - j^*$;

2) що $x \in (0, 1)^{n-1}$, але такого, у двійковому поданні якого найменш значущий біт дорівнює одиниці (x_0), як кандидатуру на i найбільш значущих бітів таємного множника d, тобто:

$$x = (x_{n-i-1} \ldots\ldots x_0)_2 - d = (d_n \ldots x_{n-i})_2;$$

3) $Q_x^{(i)} = Q^{(n)} - x\, 2^i P$, як кандидатуру на $Q_x^{(i)}$, тобто $Q_x^{(i)} - Q^{(j)}$.

Із наведеного вище випливає, що необхідно визначити такі пари i та x, щоб вони задовольняли одночасному виконанню всіх трьох умов, зазначених вище. Тобто, для кожної такої пари слід розглянути всі можливі значення $Q^{(j)*}$, що можуть бути отримані з $Q_x^{(i)}$ шляхом інвертування одного біту.

Далі шляхом симуляції роботи засобу необхідно перевірити, яке з можливих значень $Q_x^{(i)*}$ є ідентичним до отриманого із засобу помилкового результату $Q^{(n)*}$. Для цього необхідно використати операцію псевдододавання точок $x_i\, 2^{i+1} P$ при $l = 0, 2, \ldots n - i - 1$, де $x = (x_{n-i-1} \ldots x_0)_2$, $x_0 = 1$, щоб для кандидатів i, x, $Q_x^{(i)}$ отримати відповідний помилковий результат:

$$Q_x^{(n)*} = (...((Q_x^{(i)} + x_0\, 2^i\, P) + x_1\, 2^{i+1}\, P) + ...) + x_{n-i-1}\, 2^{n-1}\, P. \qquad (3.131)$$

Якщо $Q_x^{(n)*}$ є ідентичним щодо отриманого помилкового результату $Q^{(n)*}$, то отримано $i - J^*$, $Q_x^{(i)*} - Q^{(i*)}$, де $x = (x_{n-i-1}... x_0)_2 - d = (d_n... x_{n-i})_2$, тобто $n - j^*$ бітів таємного множника d. Як правило, для визначення всіх бітів таємного множника наведену процедуру необхідно повторити декілька разів. При цьому складність атаки з кожною ітерацією буде зменшуватися за рахунок використання раніше отриманої інформації.

Наведена вище спрощена модель атаки, на перший погляд, здається не зовсім реалізовною, оскільки необхідно реалізувати збій в одному із строго визначених інтервалів бітів, проте в [127] показано, як таку модель розширити за умови генерування збою у випадкові моменти часу протягом операції множення. Там же показано, що для достатньо великої кількості обчислень зі збоєм i ймовірність успішної реалізації такої атаки стає прийнятною.

3.8. МЕТОДИКА ПОРІВНЯЛЬНОГО АНАЛІЗУ СТАНДАРТІВ ЕЦП ЗА ІНТЕГРАЛЬНИМ КРИТЕРІЄМ

Одним із найважливіших і одночасно недостатньо вирішених, є завдання порівняння ЕЦП, різних алгоритмів, розмірів i за різних обмежень. Під критерієм розумітимемо ознаку, на основі якої здійснюється оцінка, визначення або класифікація чого-небудь, тобто по суті розумітимемо критерій оцінки. Попередні дослідження дозволяють зробити висновок, що порівняння ЕЦП можна здійснити з використанням двох складових: безумовного й умовного критеріїв. Оцінку ЕЦП виконуватимемо в 2 етапи. На першому етапі перевірятимемо їх на відповідність безумовним критеріям. Порівняння алгоритмів ЕЦП пропонується проводити методом аналізу ієрархій [99, 176–178].

Як алгоритми ЕЦП для порівняння пропонується вибрати такі: ECSS [27], ECDSA [15, 16, 34], EC-GDSA [15, 16, 34], EC-KCDSA [15, 16, 34], ДСТУ 4145-2002 [35], ГОСТ Р 34.10-2001 [47].

3.8.1. Спрощений опис методу ієрархій

При застосуванні методу аналізу ієрархій попарні порівняння здійснюються відносно їх впливу (ваги чи інтенсивності) на загальну характеристику системи. Парні порівняння приводять до квадратної матриці, що має вигляд:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

Ця матриця має властивість зворотної симетричності, тобто $a_{ji} = 1/a_{ij}$.

Правила заповнення квадратних матриць попарних порівнянь наведені у підрозділі 3.1. Для отримання кожної матриці експерт виносить $n(n-1)/2$ суджень (тут n – порядок матриці попарних порівнянь). Приклад формування матриці попарних порівнянь також наведено у підрозділі 3.1.

При практичному виконанні попарних порівнянь необхідно відповісти на такі питання: який із двох порівнюваних елементів є важливішим або має більший вплив, який більш імовірний і який кращий. У процесі порівняння, як правило, визначають який із критеріїв важливіший, а при порівнянні альтернатив відносно критерію – яка з них більш імовірна або краща. Парні порівняння проводяться в межах переваги одного елемента над іншим. Результати судження проводять у межах дев'ятибальної шкали згідно з таблицею 3.3. Правомірність такої шкали доведено теоретично. Більш детально правила використання шкали та її заповнення наведено у підрозділі 3.1.

Потім із групи матриць попарних порівнянь формується набір локальних пріоритетів, що й виражають відносний вплив множини елементів на елемент рівня парних порівнянь, який знаходиться зверху. Обчислюється відносна вага, величина, цінність, бажаність або ймовірність появи кожного окремого об'єкта через розв'язування матриць. Для цього необхідно обчислити множину власних векторів для кожної матриці, а потім нормалізувати результат до одиниці. Найбільш простим методом вирішення задачі є знаходження середнього геометричного. Наприклад, обчислити середнє геометричне можна шляхом перемноження всіх елементів у кожному рядку з наступним добуванням кореня n-го ступеня, де n – кількість елементів рядка матриці:

$$q_j^{(r-1)} = \sqrt[n]{(v_j^{(r)}/v_1^{(r)}) \times (v_j^{(r)}/v_2^{(r)}) \times \cdots \times (v_j^{(r)}/v_n^{(r)})},$$

де r – рівень ієрархії для матриці, відносно якої виконується розрахунок, n – кількість елементів у j рядку.

Далі отриманий таким чином стовпець нормалізується способом ділення кожного числа на суму всіх чисел:

$$\gamma_j^{(r-1)} = \frac{q_j^{(r-1)}}{\sum_{i=1}^{t_r} q_i^{(r-1)}}.$$

Може бути застосовано й інший спосіб, що полягає в нормалізації кожного стовпця матриць, а потім усередненні кожного рядка. У цьому випадку можна визначити не тільки порядок пріоритетів кожного окремого елемента, але й величину його пріоритету.

Після цього з усіх нормованих значень формуються проміжні матриці, а потім здійснюється згортання ієрархії шляхом перемноження проміжної матриці на нормований стовпець верхнього рівня. Згортання виконується до того моменту, поки не будуть отримані глобальні значення ступеня переваги однієї альтернативи над іншою.

3.8.2. Безумовні критерії оцінки ЕЦП

До безумовних критеріїв відноситимемо ті критерії, виконання яких для ЕЦП, заснованих на криптографічних перетвореннях у групі точок ЕК, є обов'язковим.

Проведений аналіз стану застосування еліптичних кривих [15, 16, 34], розробки й оцінки властивостей криптографічних перетворень у групі точок ЕК [30–37], досягнуті результати в практичному вирішенні завдань криптоаналізу та реалізації різних атак [99] дозволяють як основні вибрати такі безумовні критерії оцінки [див. 3.1]:

Надійність математичної бази, у сенсі практичної відсутності можливостей здійснювати атаки типу «Універсальне розкриття» за рахунок недосконалості математичного апарату групи точок еліптичних кривих або слабкостей, які можуть бути закладені за рахунок специфічних властивостей загальних параметрів і ключів (критерій $W_{\delta 1}$);

Практична захищеність криптографічних перетворень у групі точок ЕК від силових і аналітичних атак, яка досягається за рахунок вибору розмірів загальних параметрів і ключів (критерій $W_{\delta 2}$);

Реальна захищеність від усіх відомих і потенційно можливих криптоаналітичних атак, де під захищеністю розуміють той факт, що всі відомі криптоаналітичні атаки типу «Повне розкриття» мають експоненціальну складність I_{ec}, а критерієм незахищеності – субекспоненціальний I_{ce} (критерій $W_{\delta 3}$);

Статистична безпечність криптографічного перетворення в групі точок ЕК, під якою розуміють статистичну незалежність результату криптографічного перетворення, тобто виходу від входу (критерій $W_{\delta 4}$);

Теоретична захищеність криптографічного перетворення, у якому використовуються загальні параметри з відповідними властивостями й довжинами, при яких не існують аналітичні атаки, складність яких менше, ніж складність атаки типу «Повне розкриття» (критерій $W_{\delta 5}$);

Відсутність слабких особистих ключів, за яких складність криптоаналітичних атак типу «Повне розкриття» й «Універсальне розкриття» менша, ніж складність атаки «Повне розкриття» для інших особистих ключів (критерій $W_{\delta 6}$).

Прийняті складності прямого $I_{пр}$ та зворотного $I_{зв}$ криптографічних перетворень, коли вони мають поліноміальний характер і *не перевищують* допустимих величин $I_{пр}'$ і $I_{зв}'$ (критерій $W_{\delta 7}$).

Як результат інтегральним безумовним критерієм відбору є логічне значення так/ні (1/0), що обчислюється на основі значень часткових безумовних критеріїв

$$(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}) \in (1,0). \qquad (3.132)$$

У цілому, функцію відповідності ЕЦП для вказаних умов можна записати у вигляді

$$f_{фв}() = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5} \wedge W_{\delta 6} \wedge W_{\delta 7},$$

де символ «∧» позначає операцію кон'юнкції булевих змінних. Зрозуміло, що функції відповідності ЕЦП відповідають вимогам, якщо

$$f_{фв}() \in (0,1).$$

Таким чином, інтегральний критерій дозволяє лише встановити факт відповідності чи невідповідності такого ЕЦП безумовним вимогам.

3.8.3. Умовні критерії оцінки ЕЦП

Якісне та кількісне порівняння криптографічних перетворень у групі точок ЕК можна здійснити, використовуючи безпосередньо метод аналізу ієрархій.

Виберемо як умовні критерії оцінки ЕЦП такі часткові критерії (табл. 3.10).

Таблиця 3.10. **Умовні часткові критерії оцінки ЕЦП**

Критерії	Позначення
Можливість та умови вільного поширення й застосування міжнародного або національного стандарту криптографічних перетворень у групі точок еліптичної кривої в Україні з урахуванням нормативно-правових актів України на експорт, імпорт і обмеження на його застосування	W_{y1}
Рівень довіри до міжнародного або національного стандарту криптографічного перетворення в групі точок еліптичної кривої, що визначається результатами досліджень і степенем поширення застосування та визнання в різних державах і міжнародно визнаних системах	W_{y2}
Перспективність застосування міжнародного або національного стандарту в Україні з урахуванням визнання та застосування перспективних інформаційно-телекомунікаційних систем та інформаційних технологій тощо	W_{y3}
Тимчасова та просторова складності апаратної, апаратно-програмної та програмної реалізацій засобів ЕЦП та управління й сертифікації ключів тощо	W_{y4}
Можливість і умови застосування стандартів з різними значеннями загально-системних параметрів і ключів, методами виготовлення та обслуговування сертифікатів відкритих ключів тощо	W_{y5}
Степінь гнучкості ЕЦП з точки зору використання в різних додатках, за різних вимог та обмежень, у різних умовах, степінь уніфікації та стандартизації тощо	W_{y6}
Рівень захищеності при реалізації різних видів загроз, за різних умов здійснення криптоаналітичних атак і відхилення властивостей загальних параметрів від визначених тощо	W_{y7}

3.8.4. Порівняння алгоритмів ЕЦП

Проведемо аналіз відповідності алгоритмів ЕЦП безумовним критеріям. Результати цього аналізу подані в таблиці 3.11.

Таблиця 3.11. **Результати порівняння відносно безумовних критеріїв**

Критерій ЕЦП	W_{61}	W_{62}	W_{63}	W_{64}	W_{65}	W_{66}	W_{67}	W_6
ECSS	1	1	1	1	1	1	1	1
ECDSA	1	1	1	1	1	1	1	1
EC-GDSA	1	1	1	1	1	1	1	1
EC-KCDSA	1	1	1	1	1	1	1	1
ДСТУ 4145-2002	1	1	1	1	1	1	1	1
ГОСТ Р 34.10-2001	1	1	1	1	1	1	1	1

Тепер порівняємо алгоритми ЕЦП відносно умовних критеріїв, для цього побудуємо дерево цілей (рис. 3.1).

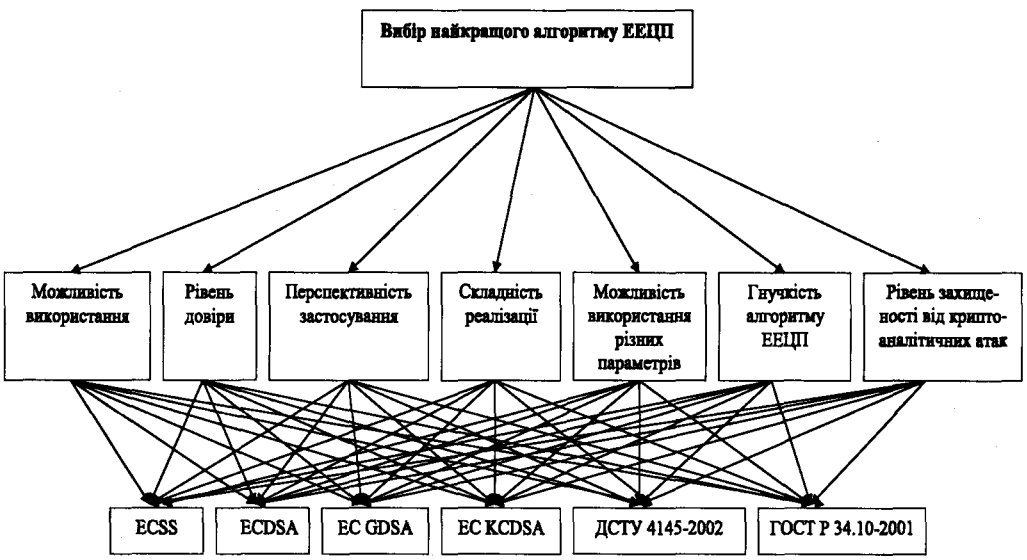

Рис 3.1. Дерево цілей

Оцінимо внесок кожного критерію в загальну мету, для цього побудуємо таблицю 3.12.

Таблиця 3.12. **Внесок критеріїв у досягнення загальної мети, матриця попарних порівнянь**

	W_{y1}	W_{y2}	W_{y3}	W_{y4}	W_{y5}	W_{y6}	W_{y7}	q_j	r_j
W_{y1}	1	1/6	4	1/4	1/2	1/3	1/7	0,4539	0,0461
W_{y2}	6	1	4	5	4	3	1/7	2,1403	0,1990
W_{y3}	1/4	1/4	1	3	2	1/2	1/7	0,5962	0,0554
W_{y4}	4	1/5	1/3	1	1/4	1/4	1/7	0,4219	0,0392
W_{y5}	2	1/4	1/2	4	1	1/3	1/7	0,6473	0,0602
W_{y6}	3	1/3	2	4	3	1	1/7	1,1925	0,1109
W_{y7}	7	7	7	7	7	7	1	5,3011	0,4930

Відношення узгодженості матриці дорівнює 14,762, що лежить у межах норми.

Тепер зробимо оцінку кожного критерію. Для цього побудуємо матрицю попарних порівнянь відносно порівнюваних алгоритмів ЕЦП для кожного критерію.

Таблиця 3.13. **Матриця попарних порівнянь критерію W_{y1}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р34.10-2001	q_j	r_j
ECSS	1	1/3	1/3	1/3	1/6	1/7	0,3097	0,0409
ECDSA	3	1	1	1	1/3	3	1,2009	0,1585
EC-GDSA	3	1	1	1	1/3	3	1,2009	0,1585
EC-KCDSA	33	1	1	1	1/3	3	1,2009	0,1585
ДСТУ 4145-2002	66	3	3	3	1	5	3,0531	0,4030
ГОСТ Р 34.10-2001	77	1/3	1/3	1/3	1/5	1	0,6107	0,0806

Відношення узгодженості дорівнює 4,5904.

Таблиця 3.14. **Матриця попарних порівнянь критерію W_{y2}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/4	1/5	1/6	1/2	1/3	0,3340	0,0417
ECDSA	4	1	1/3	1/4	1/3	1/3	0,5774	0,0721
EC-GDSA	5	3	1	1/3	2	3	1,7627	0,2200
EC-KCDSA	6	4	3	1	5	5	3,4878	0,4354
ДСТУ 4145-2002	2	3	1/2	1/5	1	2	1,0309	0,1287
ГОСТ Р 34.10-2001	3	3	1/3	1/5	1/2	1	0,8182	0,1021

Відношення узгодженості дорівнює 6,6479.

Таблиця 3.15. **Матриця попарних порівнянь критерію W_{y3}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/6	1/6	1/6	1/4	1/4	0,2572	0,0321
ECDSA	6	1	1/4	1/4	1/2	1/2	0,6740	0,0840
EC-GDSA	6	4	1	1	3	4	2,5698	0,3203
EC-KCDSA	6	4	1	1	4	4	2,6960	0,3361
ДСТУ 4145-2002	4	2	1/3	1/4	1	1	0,9347	0,1165
ГОСТ Р 34.10-2001	4	2	1/4	1/4	1	1	0,8909	0,1110

Відношення узгодженості дорівнює 3,9119.

Таблиця 3.16. **Матриця попарних порівнянь критерію W_{y4}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	3	4	4	2	3	2,5698	0,3558
ECDSA	1/3	1	3	4	2	2	1,5874	0,2198
EC-GDSA	1/4	1/3	1	3	1/2	2	0,7937	0,1099
EC-KCDSA	1/4	1/4	1/3	1	1/3	1/3	0,3637	0,0504
ДСТУ 4145-2002	1/2	1/2	2	3	1	2	1,2009	0,1663
ГОСТ Р 34.10-2001	1/3	1/2	1/2	3	1/2	1	0,7071	0,0979

Відношення узгодженості дорівнює 5,4438.

Таблиця 3.17. **Матриця попарних порівнянь критерію W_{y5}**

	ECSS	EC-DSA	EC-GDSA	EC-KCD-SA	ДСТУ 4145-2002	ГОСТ Р34.10-2001	q_j	r_j
ECSS	1	1	1	1	1	1	1,0000	0,1667
ECDSA	1	1	1	1	1	1	1,0000	0,1667
EC-GDSA	1	1	1	1	1	1	1,0000	0,1667
EC-KCD-SA	1	1	1	1	1	1	1,0000	0,1667
ДСТУ 4145-2002	1	1	1	1	1	1	1,0000	0,1667
ГОСТ Р 34.10-2001	1	1	1	1	1	1	1,0000	0,1667

Відношення узгодженості дорівнює 0,0000.

Таблиця 3.18. **Матриця попарних порівнянь критерію W_{y6}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	1/2	1/2	1/2	1	1	0,7071	0,1067
ECDSA	2	1	1	1	2	2	1,4142	0,2135
EC-GDSA	2	1	1	1/2	3	3	1,4422	0,2177
EC-KCDSA	2	1	2	1	3	3	1,8171	0,2743
ДСТУ 4145-2002	1	1/2	1/3	1/3	1	1	0,6934	0,1047
ГОСТ Р 34.10-2001	1	1/2	1/3	1/3	1	1	0,5503	0,0831

Відношення узгодженості дорівнює 2,3867.

Таблиця 3.19. **Матриця попарних порівнянь критерію W_{y7}**

	ECSS	EC-DSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001	q_j	r_j
ECSS	1	2	1/3	1/3	1/3	1/3	0,5396	0,0735
ECDSA	1/2	1	1/5	1/5	1/3	1/3	0,3612	0,0492
EC-GDSA	3	5	1	1/2	2	2	1,7627	0,2400
EC-KCDSA	3	5	2	1	3	3	2,5423	0,3461
ДСТУ 4145-2002	3	3	1/2	1/3	1	1	1,0699	0,1457
ГОСТ Р 34.10-2001	3	3	1/2	1/3	1	1	1,0699	0,1457

Відношення узгодженості дорівнює 2,9307.

Для обчислення результуючого вектора пріоритетів перемножимо вектор пріоритетів 1-го рівня та матрицю набутих значень 1-го рівня:

$$\begin{pmatrix}0.0461\\0.1990\\0.0554\\0.0392\\0.0602\\0.1109\\0.4930\end{pmatrix}\times\begin{pmatrix}0.0409 & 0.0417 & 0{,}0321 & 0.3538 & 0.1667 & 0.1067 & 0.0735\\0.1585 & 0.0721 & 0{,}0840 & 0.2198 & 0.1667 & 0.2135 & 0.0492\\0.1585 & 0.2200 & 0{,}3203 & 0.1099 & 0.1667 & 0.2177 & 0.2400\\0.1585 & 0.4354 & 0{,}3361 & 0.0504 & 0.1667 & 0.2743 & 0.3461\\0.4030 & 0.1287 & 0{,}1165 & 0.1663 & 0.1667 & 0.1047 & 0.1457\\0.0806 & 0.1021 & 0{,}1110 & 0.0979 & 0.1667 & 0.0831 & 0.1457\end{pmatrix}=\begin{pmatrix}0{,}0839\\0{,}0929\\0{,}2256\\0{,}3256\\0{,}1506\\0{,}1251\end{pmatrix}$$

3.8.5. Аналіз отриманих результатів порівняння

Розглянемо чисельні результати, отримані в попередньому розділі. Досліджувані алгоритми електронного цифрового підпису, засновані на перетвореннях у групі точок еліптичної кривої, можна розташувати за місцями, які вони зайняли за результатами порівняння (1 – найкращий, 6 – найгірший).

1. EC-KCDSA (0,3256)
2. EC-GDSA (0,2256)
3. ДСТУ 4145-2002 (0,1506)
4. ГОСТ Р 34.10-2001 (0,1251)
5. ECDSA (0,0929)
6. ECSS (0,0839)

Таким чином, ЕЦП згідно з ISO/IEC 15946-2 (EC KCDSA та EC GCDSA) за інтегральним показником мають найбільші переваги. ДСТУ 4145-2002 отримав, на наш погляд, дещо занижені оцінки, що пов'язано з недостатнім рівнем досліджень, відповідних публікацій, відсутністю заявок про вихід на міжнародний рівень тощо.

3.9. ПОРІВНЯННЯ ЕЦП З ВИКОРИСТАННЯМ МЕТОДУ ВИЗНАЧЕННЯ ВАГОВИХ КОЕФІЦІЄНТІВ НА ОСНОВІ ФУНКЦІЇ ВТРАТИ ЕФЕКТИВНОСТІ СИСТЕМ

У разі коли отримати дані про важливість параметрів порівнюваних систем з використанням неформальних методів неможливо, необхідно використовувати формалізовані методи. До них належить метод, що базується на визначенні вагових коефіцієнтів з використанням функції втрати ефективності системи [177–179]. У цьому випадку отримати деяке уявлення про області можливих значень вагових коефіцієнтів можна шляхом вивчення впливу вагових коефіцієнтів на величину узагальнених оцінок ефективності.

3.9.1. Метод визначення вагових коефіцієнтів

Розглянемо один із методів визначення вагових коефіцієнтів, а також окремих та узагальнених системних показників, а саме метод оцінки розкиду загальносистемних показників [179].

Нехай є k систем $S^{(1)}$, $S^{(2)}$, ..., $S^{(k)}$, що підлягають порівнянню. Кожна з цих систем може бути схарактеризована набором параметрів $A = \{\alpha_1, \alpha_2, ..., \alpha_n\}$. Для кожної системи будь-який параметр $\alpha_i, i = \overline{1,n}$ та $\alpha_i \in A$ може приймати своє значення:

$$S^{(1)} \to A^{(k)} = \left\{\alpha_1^{(1)}, \alpha_2^{(1)}, ..., \alpha_n^{(1)}\right\} \tag{3.133}$$

$$S^{(k)} \to A^{(k)} = \left\{\alpha_1^{(k)}, \alpha_2^{(k)}, ..., \alpha_n^{(k)}\right\}.$$

Порівняння систем виконується шляхом обчислення та подальшого порівняння часткових і системних показників.

Часткові показники характеризують ефективність системи з точки зору виконання деякої функціональної задачі. Частковий показник має вигляд:

$$\gamma_j = \sum_{i=1}^{l_j} \rho_{ij} \eta_{ij}^{(k)}, \tag{3.134}$$

де ρ_{ij} – ваговий коефіцієнт параметра в групі параметрів, які характеризують j-у функціональну задачу;

$\eta_{ij}^{(k)}$ – вказує на значення параметра k-ї системи.

Узагальнена оцінка системи визначається як

$$\Gamma^{(k)} = \sum_{j=1}^{l} \beta_j \gamma_j^{(k)}, \tag{3.135}$$

де β_j – ваговий коефіцієнт часткового показника (по суті, функціональної задачі);

$\gamma_{ij}^{(k)}$ – значення часткового показника для k-ї системи.

Метод, що розглядається, дозволяє визначити:

– нормовані значення параметрів системи η_{ij};

– вагові коефіцієнти параметрів ρ_{ij};

– вагові коефіцієнти функціональних задач β_j;

– без залучення експертів i, у кінцевому результаті, обчислити узагальнений системний показник.

Отже, розглянемо порядок розрахунку вагових коефіцієнтів і узагальненого системного показника.

Вихідна множина параметрів A піддається аналізу та розбивається на групи, які характеризують виконання окремих функціональних задач. Для проведення аналізу можна використовувати різні методи декомпозиції. За результатами аналізу отримаємо таблицю 3.20.

Таким чином, вихідна множина розбита на j груп, і кожна група має i параметрів.

2. У кожній групі параметрів визначаються параметри, які підвищуються та понижуються.

Параметром, який підвищується, $\alpha_{ij\max}$, називається параметр, підвищення значення якого призводить до підвищення ефективності системи. Тобто це параметр, для якого правильним є твердження «що більше, то краще».

Таблиця 3.20. **Результати оцінок порівняння**

№ групи j	№ $_i$ парам. у гр. i	$\alpha_{ij}^{(1)}$	$\alpha_{ij}^{(2)}$	$\alpha_{ij}^{(k)}$	$\alpha_{ij\max}$ $\alpha_{ij\min}$
1	1	$\alpha_{11}^{(1)}$	$\alpha_{11}^{(2)}$	$\alpha_{11}^{(k)}$	
	2	$\alpha_{21}^{(1)}$	$\alpha_{21}^{(2)}$	$\alpha_{21}^{(k)}$	
	3	$\alpha_{31}^{(1)}$	$\alpha_{31}^{(2)}$	$\alpha_{31}^{(k)}$	
2	1				
	2	$\alpha_{i2}^{(1)}$	$\alpha_{i2}^{(2)}$	$\alpha_{i2}^{(k)}$	
	i				
j	1				
	2	$\alpha_{ij}^{(1)}$	$\alpha_{ij}^{(2)}$	$\alpha_{ij}^{(k)}$	
	i				

Параметром, який понижується, $\alpha_{ij\max}$, називається параметр, пониження значення якого призводить до підвищення ефективності системи. Тобто для нього правильним є твердження «що менше, то краще».

Далі для кожного параметра, що підвищується, серед усіх параметрів визначається

$$\alpha_{ij\max} = \max_k \alpha_{ij}^{(k)}, \tag{3.136}$$

аналогічно

$$\alpha_{ij\min} = \min_k \alpha_{ij}^{(k)}.$$

Отримані дані заносяться в останній стовпчик табл. 3.20.

Визначаються нормовані значення параметрів. Як видно з виразу (3.21), для визначення часткового показника необхідно згорнути всі значення параметрів. Однак у явному вигляді це зробити неможна, оскільки параметри мають різний фізичний зміст і розмірність. Частковий же показник γ_i – величина безрозмірна. Саме з цієї причини зробимо нормування значень параметрів. Нормування параметрів виконується у відповідності з виразом

$$\eta_{ij}^{(k)} = \begin{cases} \dfrac{\alpha_{ij}^{(k)}}{\alpha_{ij\max}} \\ \dfrac{\alpha_{ij\min}}{\alpha_{ij}^{(k)}} \end{cases} \tag{3.137}$$

у якому обчислення $\dfrac{\alpha_{ij}^{(k)}}{\alpha_{ij\max}}$ виконується для підвищуваних параметрів, а $\dfrac{\alpha_{ij\min}}{\alpha_{ij}^{(k)}}$ – для понижуваних параметрів.

Результати нормування заносяться в табл. 3.21.

Таблиця 3.21. **Результати нормування оцінок**

№ гр. j	*№ парам. у гр. j*	$\eta_{ij}^{(1)}$	$\eta_{ij}^{(2)}$	$\eta_{ij}^{(k)}$	$\overline{\eta_{ij}}$	$\Delta\overline{\eta_{ij}}$	d_{ij}	ρ_{ij}
1	1 2 3	$\eta_{11}^{(1)}$. $\eta_{31}^{(1)}$						
2	1 2 *j*							
j	1 2 *j*							

Потім виконуємо обробку значень, поданих у таблиці 3.21.

Далі визначається середнє значення кожного нормованого параметра:

$$\overline{\eta_{ij}} = \frac{1}{m}\sum_{k=1}^{m}\eta_{ij}^{(k)}, \tag{3.138}$$

де m – кількість порівнюваних систем, $k = \overline{1,m}$

Обчислюється середнє значення розкиду кожного нормованого параметра:

$$\Delta\overline{\eta_{ij}} = \frac{1}{m}\sum_{k=1}^{m}\left|\eta_{ij}^{(k)} - \overline{\eta_{ij}}\right|. \tag{3.139}$$

Величина (3.139) характеризує відхилення параметрів систем від середнього значення чи розмах параметрів.

Обчислюється нормоване значення розкиду:

$$d_{ij} = \frac{\Delta\overline{\eta_{ij}}}{\overline{\eta_{ij}}}. \tag{3.140}$$

Далі обчислюється нормоване значення вагових коефіцієнтів за кожною групою параметрів:

$$\rho_{ij} = \frac{d_{ij}}{\sum_{i=1}^{l_7} d_{ij}}, \tag{3.141}$$

де l_7 – кількість параметрів у j-й групі.

У цілому, вище визначено вагові коефіцієнти параметрів. Фізичний сенс коефіцієнта полягає в тому, що його значення залежить від розкиду параметрів. Тобто якщо значення одного й того самого параметра для різних систем має значний розкид, то цей параметр і отримує більшу вагу при порівнянні систем. Якщо ж значення одного й того самого параметра для всіх систем однакове, то цей параметр має нульову вагу і при порівнянні систем є несуттєвим. Дійсно, якщо два алгоритми ЕЦП мають одну й ту саму складність підпису, то за цим параметром їх немає сенсу порівнювати, тобто вони рівнозначні.

Наприкінці обчислюється значення часткових показників ефективності за кожною групою параметрів:

$$\gamma_j^{(k)} = \sum_{i=1}^{l_i} \rho_{ij} \eta_{ij}^{(k)} . \qquad (3.142)$$

Отримані результати можна звести в таблицю 3.22.

Таблиця 3.22. **Часткові показники ефективності**

№ системи k / № групи j	$S^{(1)}$	$S^{(2)}$	$S^{(k)}$
1	$\gamma_1^{(1)}$	$\gamma_1^{(2)}$	$\gamma_1^{(k)}$
2			
j	$\gamma_j^{(1)}$	$\gamma_j^{(2)}$	$\gamma_j^{(k)}$

Таким чином, розглянута методика дозволяє отримати часткові показники ефективності без залучення експертів.

Розглянемо знову вираз (3.135). Для розрахунку узагальненого системного показника нам необхідно розрахувати вагові коефіцієнти β_j кожної функціональної задачі, яка характеризується своїм набором параметрів.

Визначення вагових коефіцієнтів будемо здійснювати використовуючи такі припущення.

Якщо вибрана сукупність вагових коефіцієнтів $B = \{\beta_1, \beta_2, ..., \beta_j\}$ доставляє максимум оцінкам ефективності всіх систем

$$F^{(k)}(B) = \max \Gamma^{(k)}(B) \qquad (3.143)$$

і мінімум – оцінкам решти систем

$$\Gamma^{(m)}(B) = \min \Gamma^{(m)}(B), \; m \neq k, \qquad (3.144)$$

то в цьому випадку система, що має максимум, перебуває виключно в сприятливих умовах, тобто порівняння систем необхідне.

При цьому коефіцієнти B повинні бути такими, щоб за узагальненою оцінкою ефективності $\Gamma^{(k)}(B)$ системи знаходились у відносно рівних умовах чи, у будь-якому випадку, жодна з них не повинна знаходитися в явно привілейованому положенні.

Для кількісної оцінки умов порівняння систем уведемо функцію втрат ефективності k-ї системи:

$$\theta^{(k)} = 1 - \frac{\Gamma^{(k)}}{\max_\beta \Gamma^{(k)}}, \qquad (3.145)$$

Причому функція (3.145) характеризує ступінь наближення ефективності системи при даних β до максимально можливої за будь-яких значень β.

Далі шляхом обчислення розкиду функцій втрат ефективності на основі функції (3.145) можна проводити дослідження допустимих областей значень вагових коефіцієнтів. Для цього для кожної фіксованої сукупності значень вагових

коефіцієнтів необхідно знайти максимальні й мінімальні значення функції втрат ефективності та побудувати функцію ρ (B) вигляду

$$\rho(B) = \max_k \theta^{(k)} - \min_k \theta^{(k)}. \qquad (3.146)$$

Ця функція (3.146) характеризує величину максимального розкиду. Із (3.146) можна визначити діапазон вагових коефіцієнтів, за якого розкид втрат ефективності систем (чи розкид узагальнених системних показників) не перевищить деякої величини або набуде максимального значення.

3.9.2. Методика порівняння ЕЦП

Розглянемо методику розрахунку вагових коефіцієнтів.

Нехай є j груп параметрів. Обчислимо вагові коефіцієнти для кожної групи параметрів за умови наявності значень γ_j.

Обчислимо вагові коефіцієнти для першої групи параметрів. Для цього β_1 будемо змінювати з деяким кроком у межах від 0,1 до 0,9 при дотриманні умов нормування

$$\sum_{i=1}^{l} \beta_j = 1 \qquad (3.147)$$

де l – число груп параметрів.

Для кожної сукупності β визначимо значення узагальнених системних показників усіх систем відповідно до виразу:

$$\Gamma^{(k)} = \sum_{j=1}^{l} \beta_j \gamma_j^{(k)}. \qquad (3.148)$$

Потім розрахуємо значення $\theta^{(k)}$, використовуючи вираз (3.145) і значення $\rho(B_1)$ згідно з (3.146).

За отриманими результатами будуємо графіки функції розкиду ρ(B) (рис. 3.2).

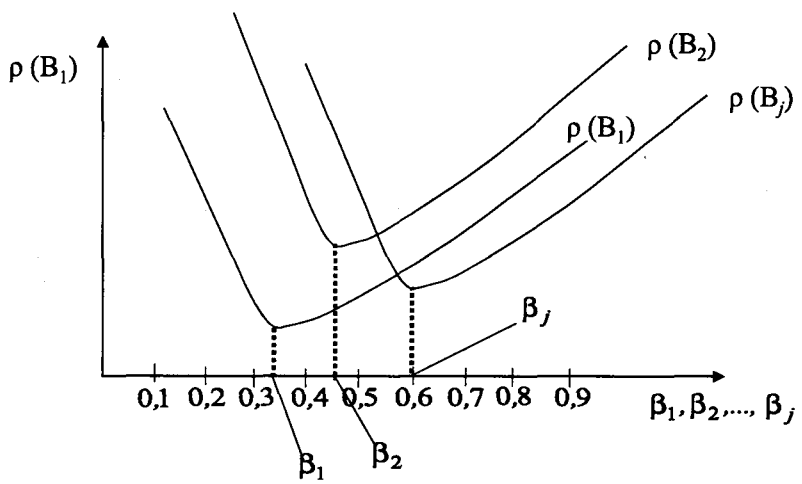

Рис. 3.2. Функції розкиду ρ (B)

Далі знаходимо значення β_1, за якого функція $\rho(\beta_j)$ набуває мінімального значення, а β_1 приймається як ваговий коефіцієнт.

Аналогічно зробимо для $\beta_2, ..., \beta_j$.

Для остаточного визначення коефіцієнтів виконаємо їх нормування. Оскільки отримані значення β не відповідають умові (3.147), то

$$\hat{\beta}_j = \frac{\beta_j}{\sum_{j=1}^{l} \beta_j}. \tag{3.149}$$

Значення узагальнених системних показників визначаються як

$$\hat{\Gamma}^{(k)} = \sum_{j=1}^{l} \hat{\beta}_j \gamma_j^{(k)}. \tag{3.150}$$

Найкращою системою вважається та, для якої

$$\Gamma_{opt} = \max \hat{\Gamma}_k. \tag{3.151}$$

Таким чином, для розв'язання задач порівняння ЕЦП може застосовуватись метод визначення вагових коефіцієнтів на основі функції втрати ефективності систем. Цей метод не вимагає залучення експертів до обробки результатів, що є суттєво важливим. У той же час при застосуванні методу ієрархій Сааті необхідне залучення деякої множини експертів. Попередні дослідження й застосування обох методів та отримані в результаті застосування відповідних методик результати збігаються.