Розділ 2

СУТНІСТЬ ТА ОСНОВИ ЗАСТОСУВАННЯ ЕЦП

2.1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІСНУЮЧИХ ЕЦП ТА ГЕШ-ФУНКЦІЙ

Загально визнано, що такі основні послуги систем криптографічного захисту, як цілісність, справжність і неспростовність відправника можуть бути забезпечені за умови обов'язкового використання ЕЦП. Обов'язковим елементом, що використовується в ЕЦП, є геш-функція, за допомогою якої обчислюється геш-значення від електронних даних і взагалі інформації, що підписуються. На практиці залежно від математичного апарату, що застосовується в ЕЦП, історично знайшли застосування три класи цифрових підписів: RSA ЕЦП, що базується на перетворенні в кільці; Ель-Гамаля DSA перетворення, що базується на перетворенні в полі Галуа; Ель-Гамаля ЕС перетворення, що ґрунтується на перетвореннях у групі точок еліптичних кривих. У перспективі можуть бути прийняті як стандарти ЕЦП, що можуть ґрунтуватися на спарюванні точок еліптичних кривих та використанні як відкритих ключів ідентифікаторів, тобто системи на ідентифікаторах. У таблиці 2.1 наведено перелік основних стандартів ЕЦП залежно від математичного апарату, що використовується в них при перетвореннях.

Таблиця 2.1. **Основні стандарти ЕЦП**

RSA	Ель-Гамаля DSA	Ель-Гамаля EC
X 9.31 ISO 11166	X 9.30-1991 ГОСТ Р 34.10-94–1995 ГОСТ 34.310-95–1996	X 9.62–2001, ISO/IEC 15946-2 : 2001 (ISO/IEC 14888-3 : 2006), ISO/IEC 15946-4 : 2004 (ISO/IEC 9796-3 : 2006), ГОСТ Р 34.10-94–2001, ДСТУ 4145–2002
FIPS 186-3 (RSA)	FIPS 186-3 (DSA)	FIPS 186-3 (ECDSA)

Функції гешування є примітивами, що використовуються в різних криптографічних додатках. Найбільш важливі застосування належать до електронного цифрового підпису та протоколів автентифікації. Можна виділити три основних підходи до побудови функцій гешування [33]:

– функції гешування, що побудовані з використанням блокових шифрів [10, 39, 41];

– функції гешування, що засновані на арифметиці з перетворенням за певним модулем [7–10, 39];

– замовлені функції гешування [10, 39, 51].

Міжнародна організація зі стандартизації ISO/IEC розробила стандарт для опису різних класів функцій гешування [39]. У частині ISO/IEC 10118-1 подано загальні визначення, вимоги та схеми функцій гешування.

У частині ISO/IEC 10118-2 визначені функції гешування, засновані на блокових шифрах у конструкції Matyas-Meyer-Oseas, коли незалежний блоковий шифр в алгоритмі MDC-2 з двома і більше функціями формує геш-значення подвоєної та потроєної довжини відповідно.

Частина ISO/IEC 10118-3 визначає три замовлених алгоритми: RIPEMD-128, RIPEMD-160 і SHA-1. Ця частина стандарту на цей час переглядається, з оцінкою нових криптографічних примітивів, що будуть прийняті як стандарти ISO. Окрім відзначених трьох алгоритмів, широкого застосування набули функції гешування: SHA-2/256, SHA-2/384, SHA-2/512 і Whirlpool.

Частина ISO/IEC 10118-4 описує MASH-1 і MASH-2 функцій гешування, що використовують арифметику з перетворенням за певним модулем. Більш детально функції гешування розглядаються у розділі 5 цієї монографії.

Основні характеристики функції гешування наведено в табл. 2.2.

Таблиця 2.2. **Характеристики функцій гешування**

Функція гешування	Клас функції	Базові перетворення	Довжина геш-значення, бітів
Whirlpool	Однонаправлена	У кінцевих полях і матрицях	512
SHA-2	Однонаправлена	Логічні й арифметичні	256, 384, 512
ГОСТ 34.311-95	Однонаправлена	Блоковий симетричний шифр	256
HAVAL	Однонаправлена	Логічні й арифметичні	128, 160, 192, 256
SHA-1	Однонаправлена	Логічні й арифметичні	160
RIPEMD-160	Однонаправлена	Логічні й арифметичні	160
MD5	Однонаправлена	Логічні й арифметичні	128
MD4	Однонаправлена	Логічні й арифметичні	128
UMAC	Однонаправлена і вироблення КАП	У кільцях	128, 64
Rijndael CBC-MAC	Вироблення КАП	Блоковий симетричний шифр	128
ГОСТ 28147-89 (режим 4)	Вироблення КАП	Блоковий симетричний шифр	64

2.2. ЕЦП ЗГІДНО З ISO 11166 ТА FIPS 186-3

У США запропоновано новий проект федерального стандарту FIPS 186-3, згідно з яким ЕЦП може виконуватися в тому числі й на основі RSA перетворення. ЕЦП на основі RSA здійснюється засобом формування спочатку відкритого підпису, що включає в себе значення геш-функції $h(M)$ від інформації (електронних даних), яка підписуються, а також необов'язково може включати ідентифікатори відправника – $I_в$, одержувача – I_o, час створення – t_c, інтервал життя – Δt та інші параметри. Відкритий підпис для вказаних даних подається далі у вигляді одного чи декількох цілих чисел:

$$\text{ВП} = (h(M), I_в, I_o, I_c, \Delta t), \tag{2.1}$$

а ЕЦП обчислюється засобом шифрування відкритого підпису ВП, тобто:

$$\text{ЦП} = \text{ВП}^{E_k} (\text{mod}\, N_j), \tag{2.2}$$

де E_k – особистий ключ ЕЦП відповідного користувача.

Модуль перетворення N є добутком двох простих чисел P та Q, тобто:

$$N_1 = P_j \cdot Q_j. \tag{2.3}$$

Усі користувачі, що володіють відкритим ключем D_k, відновлюють ВП, тобто розшифровують ЦП таким чином:

$$\text{ВП}' = \text{ЦП}^{D_k} (\text{mod}\, N_j) \tag{2.4}$$

та отримують дані вигляду (2.1).

Потім для даних M', що розглядаються, розраховується геш-значення $H(M'')$ й отримане геш-значення порівнюється зі значенням, що міститься у (2.1):

$$H(M') = H(M). \tag{2.5}$$

Якщо значення співпадають, то M' вважається цілісним і справжнім, і авторство даних підтверджується. В іншому випадку дані відкидаються.

Порядок використання RSA алгоритму для обчислення та перевірки цифрового підпису наведені в стандартах ANSI X 9.31 і PKCS #1 а також [46]. Хоча кожен із цих стандартів використовує алгоритм RSA, формат ANS X 9.31 і PKCS #1 дані, для яких обчислюється цифровий підпис, суттєво відрізняються, що робить їх невзаємозамінними.

RSA ключова пара складається з особистого ключа, який використовується для обчислення цифрового підпису, і RSA відкритого ключа, який використовується для перевірки цифрового підпису. RSA ключова пара, що призначена для цифрових підписів, повинна використовуватися тільки для цифрових підписів, але не для інших цілей (наприклад, у протоколі встановлення ключів).

RSA відкритий ключ складається з модуля N, який є результатом обчислення добутку двох позитивних простих чисел P та Q_i (тобто згідно (2.3)) та відкритого ключа D. Тому RSA відкритий ключ є парою значень (N, D) і використовується для перевірки цифрових підписів. Зазвичай вважається, що розмір RSA ключової пари дорівнює довжині модуля N у бітах (l_N).

Відповідний RSA особистий ключ складається з того самого модуля N та особистого ключа E, які залежать від N і відкритого ключа D. Тому RSA особистий ключ є парою значень (N, E) і використовується для обчислення цифрових підписів. Відзначимо, що альтернативний метод представлення (N, E) з використанням

китайської теореми про лишки допускається, як визначено в PKCS #1. За цих умов може бути підвищена швидкість обчислення та перевірки підпису. Значення простих чисел P та Q, а також особистий ключ підпису E є таємними, відносно них повинні бути забезпечені такі послуги як конфіденційність, цілісність, справжність, доступність і неспростовність. Модуль N і ключ D перевірки підпису є відкритими, але щодо них мають бути забезпечені такі послуги як цілісність, справжність, доступність і неспростовність D. Керівництво із захисту цих значень надається в стандарті США SP 800-57.

Стандарт допускає три варіанти для довжини модуля (тобто l_N): 1024, 2048 і 3072 бітів. Федеральні Урядові органи повинні використовувати один із цих варіантів. Як затверджені геш-функції необхідно використовувати алгоритми гешування, що наведені у FIPS 180-2. При цьому стійкість використовуваної геш-функції повинна відповідати або перевищувати стійкість цифрового підпису, яка визначається бітовою довжиною модуля N. Відповідні рівні стійкості для кожної довжини модуля та геш-функції наведені в NIST SP 800-57. Рекомендується, щоб стійкість захисту модуля і геш-функції були однаковими.

Більш детально генерування ключів та застосування RSA у відповідності з сучасними вимогами наведено в [46].

2.3. ЕЦП, ЩО ВИЗНАЧЕНІ У FIPS 186-1, ГОСТ 34.310-95 ТА ГОСТ Р 34.10-2001

2.3.1. Загально-системні параметри

Алгоритми ЕЦП FIPS 186-1 (DSA) та ГОСТ 34.310-95 [10, 43, 40, 51] дуже схожі та пройшли випробовування часом. Ці алгоритми продовжують застосовуватися дуже широко. Так, у FIPS 186-3 [46] передбачається продовжити використання DSA. По суті, в них використовується криптографічний алгоритм перетворення Ель-Гамаля за двома модулями P та q. Загальносистемними параметрами є $\{P, q, g\}$ для DSA або $\{P, q, a\}$ для ГОСТ 34.310-95, де P є просте «сильне» число, q – також просте число, але яке входить в канонічний розклад числа $(P-1)$, а g – первісний елемент простого поля. У таблиці 2.3 наведено вимоги щодо цих загальносистемних параметрів.

Таблиця 2.3. **Загальні параметри ЕЦП у простому полі Галуа**

DSA	ГОСТ 34.310-95
1	2
$\{P, q, g\}$	$\{P, q, a\}$
P – просте число $2^{511} < P < 2^{1024}$ і може змінюватися з кроком $\Delta l = 64$ бітів	$2^{509} < P < 2^{512}$ $2^{1020} < P < 2^{1024}$
q – просте число $2^{159} < q < 2^{160}$	$2^{255} < q < 2^{256}$

Закінчення табл. 2.3

1	2
$P-1=q\alpha_1^{x_1}, q\alpha_2^{x_2}\ldots$	
$1<g<p$	$1<a<p$
$g^q \pmod P = 1$	$a^q \pmod P = 1$

Указані загальносистемні параметри можуть бути для всіх користувачів однаковими й змінюватися дуже рідко. У FIPS 186-1 обмеження на загальні параметри інші. Алгоритми вироблення та перевірки підпису розглянемо на прикладі DSA подібного ЕЦП згідно з ГОСТ 34.310-95.

2.3.2. ЕЦП ГОСТ Р 34.10-94 та ЕЦП ГОСТ 34.310-95

Вироблення ЕЦП для ГОСТ 34.310-95 (ГОСТ Р 34.10-94)

У процесі підпису для повідомлення (даних) необхідно виробити підпис, що складається з двох цілих чисел (r, S), де r – по суті, таємний (особистий) ключ сеансу (його значення щодо кожного підпису повинне змінюватись, навіть якщо одне й те саме повідомлення підписується повторно), а S – підпис.

У DSA подібних ЕЦП попередньо має бути вироблена для кожного користувача асиметрична пара ключів (x_i, Y_i), де x_i – особистий ключ, а Y_i – відкритий ключ. Для цього, як правило, застосовується схема Діффі-Геллмана розповсюдження ключів [10, 51, 7–9]. При цьому кожен користувач формує довгостроковий особистий ключ x_i, причому

$$1 < x_i < q,$$

а потім обчислює відкритий ключ

$$Y_i = a^{x_i} \pmod p = 1. \tag{2.6}$$

З відкритого ключа, як правило, виготовляється сертифікат відкритого ключа, який у подальшому повинен бути доступний усім користувачам, які отримують підписані відповідним користувачем дані.

Обчислення ЕЦП здійснюється в такому порядку:

Для M обчислюється геш-значення $h = H(M)$, причому як геш-функція має використовуватися ГОСТ 34.311-95. Якщо $h = 0$, то вона змінюється $h = 0^{255}1$.

За допомогою випадкового або детермінованого генератора бітів генерується ключ сеансу k, причому $0 < k < q$.

Обчислюється значення $r' = a^k \pmod P$, тобто спочатку за модулем P, а потім за модулем q, відкритий ключ сеансу

$$r = r' \pmod q. \tag{2.7}$$

Далі обчислюється безпосередньо підпис:

$$S = (xr + kh) \bmod q. \tag{2.8}$$

Підписане повідомлення (дані) M мають такий вигляд – M, (r, S).

Перевіряння ЕЦП

Перевіряння ЕЦП, тобто цілісність і справжність прийнятого повідомлення M', повинне виконуватися за таких умов і в такому порядку:

1) користувачеві, що перевіряє підпис, мають бути відомі:

– підписані дані $< M', (r', S') >$;

– загальні параметри $\{P, q, a\}$ та сертифікат відкритого ключа Y_i;

2) далі необхідно перевірити цілісність, справжність і встановити авторство даних M.

Перевіряння ЕЦП виконується в такому порядку:

1) перевіряється умова, що $0 < r', S' < q$, інакше r', S' є викривленими, тому перевірку робити немає сенсу;

2) обчислюється геш-значення від даних, що перевіряються $h = H(M')$;

3) обчислюються додаткові дані:

$$V = (h)^{q-2} (\text{mod } q);$$

$$Z_1 = SV (\text{mod } q);$$

$$Z_2 = (q - r')V (\text{mod } q).$$

По суті, $V = 1/h \,(\text{mod } q) = (h)^{q-2} \,(\text{mod } q)$, тобто h та $(h)^{q-2}$ приймає зворотне до h значення в полі $F(q)$ є мультиплікативні зворотні за модулем q. Тому в наступних двох вищенаведених формулах знаходяться добутки вигляду SV та $(q - r')V$, що використовуються у формулі:

$$a^{Z_1} Y^{Z_2} = (\text{mod } p) \,(\text{mod } q) = U; \tag{2.9}$$

4) здійснюється перевірка виконання умови $U = r'$. Якщо порівняння виконується, то дані вважаються цілісними й справжніми та визнається їх авторство. Інакше дані відкидаються.

У стандарті FIPS-186 для обчислення r використовується та сама формула, що й у ГОСТ 34.310-95, а для обчислення S компоненти ЕЦП використовується така формула:

$$S = (h + xr)/k (\text{mod } P) (\text{mod } q). \tag{2.10}$$

Підписом у цьому стандарті є також пара цілих чисел (r, S).

Обґрунтування вибору цих формул можна знайти в [10].

2.3.3. ЕЦП ГОСТ 34.10-2001

Стандарт ЕЦП ГОСТ Р 34.10-94 був реалізований з використанням криптографічних перетворень у полі Галуа, перш за все у вигляді стандарту Російської федерації, а потім його розширення у вигляді міждержавного стандарту ГОСТ 34.310-95, які наслідували всі характеристики й можливості, що були досягнуті та представлені у федеральному стандарті США FIPS 186-1. З розвитком методів і засобів криптоаналізу стало зрозуміло, що стійкість проти атаки «Повне розкриття» для ЕЦП, що реалізована з використанням криптографічних перетворень у полі Галуа, носить субекспоненційний характер і має тенденцію до зменшення. По суті, вона зводиться до розв'язку порівняння (2.6) щодо особистого ключа x_i. У результаті пошуку й досліджень, на відміну від (2.6), було запропоновано особистий

ключ зв'язувати з відкритим з використанням скалярного множення в групі точок еліптичної кривої над відповідним полем Галуа, тобто обчислювати відкритий ключ з використанням операції скалярного множення [8–10, 51, 30–32].

$$Q_i = d_i \cdot G \pmod{q}, \tag{2.11}$$

де d_i – особистий ключ користувача, Q_i – відкритий ключ, G – базова точка. При застосуванні скалярного множення складність розв'язку порівняння суттєво збільшилась та набула експонентного характеру. Відповідно треба було модифікувати й перевірку підпису, увівши операцію скалярного множення. Уперше це було реалізовано в стандарті ANSI X 9.62 [44], а потім й у федеральному стандарті США FIPS 186-2 [45]. У подальшому вдосконалений таким чином стандарт ЕЦП ANSI X 9.62 (FIPS 186) позначений як ECDSA (DSA в групі точок еліптичних кривих).

На основі ГОСТ 34.310-94 за аналогією з ECDSA було обґрунтовано й розроблено проект національного стандарту в групі точок еліптичної кривої. У 2000 р. він був опублікований у [171] помилково як стандарт цифрового підпису ГОСТ 32.310-95 на еліптичних кривих. Офіційної підтримки в Україні в подальшому проект не отримав, але восени 2001 р. стало відомо, що з 01.07.2002 у Російській Федерації набуває чинності стандарт електронного цифрового підпису ГОСТ Р 32.10-2001, що ґрунтується на еліптичних кривих. Як випливає з наведеного нижче, він у частині виробки та перевіряння електронного цифрового підпису співпадає з проектом ЗАТ «ІІТ».

Алгоритми обчислення та перевіряння ЕЦП національного проекту наведено в таблиці 2.4.

Таблиця 2.4. **Алгоритми обчислення та перевіряння ЕЦП національного проекту**

Обчислення 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. Обчислити $h = H(M) \bmod (q)$ та подати у вигляді цілого числа. 2. Згенерувати випадкове $0 < k < q$. 3. Обчислити $R = k \cdot G = (x_R, y_R)$. 4. Обчислити $r = \pi(R) \bmod q = x_R \bmod q$. 5. Обчислити $S = (Xr + kh) \bmod q$	1. Перевірити що: $0 < r' < q,\ 0 < s' < q$. 2. Обчислити $h = H'(M')$ та подати у вигляді цілого числа. 3. $v = (H'(M'))^{q-2} \bmod q$. 4. $Z_1 = S \cdot v \pmod{q},\ Z_1 = (q - r') \cdot v \pmod{q}$. 5. $u = Z_1 G + Z_2 Y$. 6. $U = u_x \pmod{q}$. 7. Якщо $r' = u$, то M' цілісне та дійсне, інакше – хибне.

Алгоритми обчислення та перевіряння ЕЦП згідно з ГОСТ 34.10-2001 наведено в таблиці 2.5.

Таблиця 2.5. **Алгоритми обчислення та перевіряння ЕЦП згідно з ГОСТ 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 й справжнє або ні.
1. Обчислити $h' = H(M)$ та представити у вигляді цілого числа. 2. Обчислити $h = h' \pmod q$. 3. Згенерувати випадкове k, $0 < k < q$. 4. Обчислити $R = (kG) \bmod q = (x_R, y_R)$. 5. Обчислити $r' = x_R \pmod q$. 6. Обчислити $s' = (rd + kh) \bmod q$.	1. Перевірити, що $0 < r' < q$, $0 < s < q$. 2. Обчислити $h_1 = H(M')$ та подати у вигляді цілого числа. 3. Обчислити $\bar{h} = h_1 \pmod q$. 4. Обчислити $v = h^{-1} \pmod q$. 5. Обчислити значення $Z_1 = s \cdot v \pmod q$, $Z_2 = -r \cdot v \pmod q$. 6. Обчислити $c = (Z_1 G + Z_2 Q) \bmod q = (x_c, y_c)$. 7. Визначити $R = x_c \pmod q$. 8. Якщо $R = r'$, то підпис цілісний і справжній, інакше – ні.

Аналіз захищеності ГОСТ 34.10-2001 від існуючих загроз і можливих атак, а також порівняння властивостей і характеристик наведено в розділі 3 та [95–97, 113–115, 129–131].

2.4. ЕЦП ЗГІДНО З ISO/IEC 14888-3 (15946-2)

Наприкінці XX сторіччя було встановлено, що складність вирішення дискретного рівняння

$$Y_i = a^{X_i} \pmod P \tag{2.12}$$

відносно особистого ключа, тобто складність знаходження X, має субекспоненційний характер. Наприклад, при розмірі модуля $P = 2^{1024}$ складність із застосуванням загального решета числового поля буде складати всього приблизно 10^{28} операцій множення з числами відповідного розміру. У той же час, враховуючи сьогоднішні досягнення, розв'язання рівняння

$$Q_i = d_i \cdot G \pmod q \tag{2.13}$$

відносно d_i має експонентний характер i. Наприклад, при порядку базової точки $n = 2^{1024}$ із застосуванням ρ-методу Полларда складає приблизно 10^{153} операцій складання точок на еліптичній кривій. Таким чином, складність вирішення дискретного логарифмічного рівняння в групі точок еліптичної кривої незрівнянно вища. Це здебільшого й визначило широке застосування та прийняття відповідних стандартів криптографічних перетворень на основі перетворень у групі точок еліптичних кривих.

Враховуючи зазначене, у 1992 році в США були розпочаті роботи з модифікації алгоритму DSA використання співвідношення (2.13) при формуванні асиметричної пари ключів (d_i, Q_i). Такий перехід дав можливість згідно з поглядами того часу (та й нинішніх) забезпечити експонентну складність здійснення загрози повного розкриття, а по суті перекрити вразливість дискретного логарифма вигляду (2.12), оскільки відносно нього складність уже в той час мала субекспоненційний характер. Перший варіант модифікованого таким чином DSA підпису був прийнятий в США у вигляді стандарту ANSI X 9-62, а сам алгоритм отримав шифр ECDSA. У подальшому він був прийнятий як один із алгоритмів ЕЦП міжнародного стандарту ISO/IEC 15946-2 та набув широкого поширення у світі. У 2006 році ISO/IEC 15946-2 був відкликаний як міжнародний стандарт, а потім прийнятий як міжнародний ISO/IEC 14888-3:2006 «Інформаційні технології – Методи захисту – Цифрові підписи з додатком – Частина 3. Механізми, що базуються на дискретному логарифмі» [34]. На цей час він є чинним і широко використовується в багатьох державах. Він також включений до нового федерального стандарту США FIPS 186-3. Крім того, спочатку в ISO/IEC 15946-2, а потім і в ISO/IEC 14888-3:2006 були також включені алгоритми ЕЦП EC-GDSA та EC-KCDSA. Указані два алгоритми ЕЦП мають ряд переваг, що буде розглянуто окремо.

Стійкість усіх трьох ЕЦП базується на складності задачі логарифмування в групі точок еліптичних кривих, що визначені над деяким скінченним простим полем $F(p)$, $F(2^m)$ або $F(p^m)$.

ЕЦП або схема цифрового підпису визначаються засобом специфікації процесів генерації параметрів, обчислення цифрового підпису та перевірки цифрового підпису. Розглянемо їх детально для кожного із стандартів.

2.4.1. Загальний опис схем ЕЦП згідно з ISO/IEC 14888-3 (15946-2)

Параметри ЕЦП можна розділити на параметри домену й параметри користувачів.

Параметри домену містять параметри для визначення скінченного поля, еліптичної кривої над скінченним полем, та іншу відкриту інформацію, що є загальною й відомою або доступною всім об'єктам усередині домену. Для загальних криптографічних схем, визначених у стандарті ISO/IEC 44888-3 (ISO/IEC 15946-2), що базуються на еліптичних кривих, разом із параметрами домену необхідно визначити такі параметри:

– ідентифікатор, що використовують для позначення схеми цифрового підпису;

– ідентифікатор для геш-функції $h()$, що відображає довільні повідомлення в бітовий рядок фіксованої довжини;

– процедуру генерації параметрів користувачів.

Параметри користувачів. Кожен об'єкт має свої відкриті й особисті параметри. Параметри користувачів об'єкта A містять такі елементи:

– особистий ключ d_A;

– відкритий ключ P_A;

– (необов'язково) інша інформація, що стосується об'єкта A, та використовується під час обчислення цифрового підпису чи (або) при його перевірянні.

Процес вироблення цифрового підпису

Для вироблення цифрового підпису потрібні такі елементи даних:

– параметри домену;

– параметри користувачів підписувача A, що включають особистий ключ d_A;

– повідомлення M.

Для всіх схем, тобто ECDSA, EC-GDSA та EC-RCDSA, у процесі вироблення цифрового підпису використовуються такі процедури:

– обчислення геш-значення;

– обчислення на еліптичних кривих;

– обчислення за модулем порядку групи базової точки G.

Вихідними даними процесу вироблення цифрового підпису є пара цілих чисел (r, s), що становлять цифровий підпис повідомлення M об'єкта A.

Перед кожним обчисленням цифрового підпису об'єкт, що підписує, повинен мати в наявності та використовувати нове, таємне значення ключа сеансу. Ключ сеансу є цілим числом k в межах $1 < k < n - 1$. Реалізація схеми цифрового підпису повинна гарантувати виконання таких двох вимог [7–10, 15, 16, 36, 37, 43–47, 51]:

– ключі сеансу, що використовуються, ніколи не повинні розкриватися, оскільки в разі знання ключа сеансу та цифрового підпису, виробленого з його використанням, можна здійснити компрометацію особистого ключа цифрового підпису;

– ключі сеансів повинні бути статистично унікальні, тобто ймовірність того, що при виробленні цифрових підписів для двох різних повідомлень буде використаний однаковий ключ сеансу, є нехтовно малою. Якщо при виробленні цифрових підписів для двох різних повідомлень використовується однакове значення ключа сеансу, тоді ключ цифрового підпису можна визначити із цих двох цифрових підписів.

Процес перевіряння цифрового підпису

Для процесу перевіряння цифрового підпису потрібні такі елементи даних:

– параметри домену;

– параметри користувачів підписувача A, що містять відкритий ключ P_A, але не включають особистий ключ d_A;

– одержане повідомлення M';

– одержаний цифровий підпис повідомлення M, що представлений двома цілими числами r' та s'.

Для всіх схем процес перевіряння цифрового підпису складається з деяких або всіх таких процедур:

1) перевіряння розміру цифрового підпису;
2) обчислення геш-значення повідомлення;
3) обчислення за модулем порядку групи базової точки G;
4) обчислення на еліптичних кривих;
5) перевіряння цифрового підпису.

Якщо всі процедури проходять успішно, то цифровий підпис приймається перевірником, в іншому випадку підпис відхиляється.

2.4.2. ЕЦП згідно з ECDSA та його застосування

Схема цифрового підпису ECDSA є аналогом схеми цифрового підпису DSA на еліптичних кривих. Схема є прикладом механізму вироблення цифрового підпису з додатком. Для застосування ЕЦП повинні бути заданими параметри домену та параметри користувачів. Бітова довжина модуля n має бути більше, ніж бітова довжина вихідного значення геш-функції $h()$. Особистий та відкритий ключі об'єкта A, d_A і P_A відповідно, необхідно виробляти у відповідності з процедурою, визначеною в стандарті ISO/IEC 15946-1 та описаною в п. 6.

Вироблення цифрового підпису

Вхідними даними для процесу цифрового підпису є такі:
– параметри домену;
– особистий ключ d_A підписувача;
– повідомлення M.

Вихідними даними процесу вироблення цифрового підпису є пара $(r, s) \in F(n)^* \times F(n)^*$, що є цифровим підписом повідомлення M об'єкта A.

При підписуванні повідомлення M об'єкт A виконує такі кроки:

1) обчислення геш-значення $e = h(M)$;

2) вибір або генерування ключа сеансу – випадкового цілого числа k, що належить діапазону $\{1, ..., n-1\}$;

3) обчислення точки еліптичної кривої $(x_1, y_1) = kG$;

4) обчислення відкритого ключа сеансу $r = \pi(kG) \bmod n$;

5) обчислення значення k^{-1} у полі $F(n)$;

6) обчислення значення цифрового підпису $s = (d_A r + e)k^{-1} \bmod n$.

Якщо в процесі обчислення цифрового підпису $s = 0$ або $r = 0$, тоді процес вироблення цифрового підпису необхідно повторити з новим випадковим значенням k. Але необхідно зазначити, що ймовірність того, що $r = 0$ або $s = 0$ є надзвичайно малою, якщо k обрано випадково та згідно з вимогами, що наведені в [15, 30–32].

Окрім того, оскільки обчислене значення r не залежить від підписуваного повідомлення, конфіденційний ключ сеансу, тобто число k та відкритий ключ сеансу – число r можуть обчислюватися попередньо і надалі зберігатися й використовуватися під час вироблення цифрового підпису. Але щодо числа k, то воно має зберігатися в таємниці, оскільки його компрометація може призвести до компрометації особистого ключа d_A.

Таким чином, пара цілих чисел $(r, s) \in F(n)^* \times F(n)^*$ становить цифровий підпис повідомлення M об'єкта A.

Перевіряння цифрового підпису

Перевіряння цифрового підпису здійснюється за 4 кроки:

1) перевіряння розміру цифрового підпису;

2) обчислення геш-значення повідомлення;

3) обчислення на еліптичних кривих;

4) перевіряння цифрового підпису.

Вхідними даними для перевіряння цифрового підпису є такі:

– параметри домену;

– відкритий ключ P_A об'єкта A;

– підписане повідомлення M';

– цифровий підпис повідомлення M, що представлений двома цілими числами r' та s'.

Для перевіряння цифрового підпису повідомлення M' об'єкта A об'єктом B виконуються такі кроки:

1) перевіряння умов $0 < r' < n$ та $0 < s' < n$. Якщо одна з умов не виконується, то цифровий підпис відхиляється;

2) обчислення геш-значення $e' = h(M')$ за допомогою геш-функції $h()$;

3) обчислення оберненого в полі $F(n)$ відносно s' елемента $w = (s')^{-1} \bmod n$;

4) обчислення допоміжних даних $u_1 = e'w \bmod n$ та $u_2 = r'w \bmod n$;

5) обчислення точки еліптичної кривої $(x_1, y_1) = u_1 G + u_2 P_A$;

6) обчислення $v = \pi(x_1, y_1) \bmod n$.

Якщо $r' = v$, то перевірник повинен прийняти цифровий підпис. Якщо $r' \neq v$, то перевірник має відхилити цифровий підпис.

Особистий і відкритий ключі об'єкта A, d_A і P_A відповідно необхідно виробляти у відповідності з вимогами, що визначені в стандарті ISO/IEC 15946-1 і наведені в [30–32].

2.4.3. ЕЦП згідно з EC-GDSA та його застосування

Схема цифрового підпису EC-GDSA є прикладом механізму вироблення цифрового підпису з додатком. В узагальненому вигляді ця схема по суті розглянута у 2.4.1. Для цієї схеми бітова довжина модуля n повинна бути більшою, ніж бітова довжина вихідного значення функції гешування $h()$. Особистий і відкритий ключі об'єкта A, d_A і P_A відповідно необхідно виробляти у відповідності з процедурою, що визначена в стандарті ISO/IEC 15946-1 [30–32].

Вироблення цифрового підпису

Вхідними даними для процесу цифрового підпису є такі:

– параметри домену;

– особистий ключ d_A підписувача;

– повідомлення M.

Вихідними даними процесу вироблення цифрового підпису є пара $(r, s) \in F(n)^* \times F(n)^*$, яка є цифровим підписом повідомлення M об'єкта A.

Підписування повідомлення M об'єктом A виконується в такій послідовності:

1) обчислюється геш-значення повідомлення M;

2) вибирається чи генерується випадкове ціле число k – ключ сеансу, яке належить інтервалу $\{1, ..., n-1\}$;

3) обчислюється точка еліптичної кривої $(x_1, y_1) = kG$;

4) обчислюється значення $r = \pi(kG) \bmod n$ – відкритий ключ сеансу;

5) обчислюється значення цифрового підпису $s = (kr - e)d_A \bmod n$.

Необхідно зазначити таке: якщо в процесі вироблення цифрового підпису $s = 0$, або $r = 0$, то процес необхідно повторити з новим випадковим значенням k, починаючи з кроку 2. Необхідно зазначити, що ймовірність того, що $r = 0$ або $s = 0$ є надзвичайно малою, якщо k обрано випадково. Окрім того, оскільки значення r не залежить від підписуваного повідомлення M, число r може обчислюватися попередньо та надалі зберігатися й використовуватися під час вироблення цифрового підпису. Окрім того, щодо k – ключа сеансу необхідно забезпечувати конфіденційність, цілісність, справжність і доступність, а щодо r – його цілісність, справжність і доступність.

Перевіряння цифрового підпису

Пара цілих чисел $(r, s) \in F(n)^* \times F(n)^*$ становить цифровий підпис повідомлення M об'єкта A.

Перевіряння цифрового підпису складається з таких кроків:

1) перевіряння розміру цифрового підпису;

2) обчислення геш-значення повідомлення;

3) обчислення на еліптичних кривих;

4) перевіряння цифрового підпису.

Вхідними даними процесу перевіряння цифрового підпису є такі:

– параметри домену;

– відкритий ключ P_A об'єкта A;

– одержане повідомлення M';

– одержаний цифровий підпис повідомлення M, представлений двома цілими числами r' та s'.

Для перевіряння цифрового підпису повідомлення M' об'єкта A об'єктом B виконуються такі кроки:

1) перевіряння умов $0 < r' < n$ та $0 < s' < n$. Якщо хоч одна з умов не виконується, то цифровий підпис відхиляється.

2) обчислення геш-значення $e' = h(M')$ з використанням геш-функції $h()$ від повідомлення M'.

3) обчислення $w = (r')^{-1} \bmod n$.

4) обчислення $u_1 = e'w \bmod n$ та $u_2 = s'w \bmod n$.

5) обчислення точки еліптичної кривої $(x_1, y_1) = u_1G + u_2P_A$.

6) обчислення $w = \pi(x_1, y_1) \bmod n$.

Якщо $r' = v$, то перевірник повинен прийняти цифровий підпис. Якщо $r' \neq v$, то перевірник має відхилити цифровий підпис.

2.4.4. ЕЦП згідно з KCDSA та його застосування

Схему цифрового підпису EC-KCDSA наведено в [15, 34]. Алгоритми обчислення та перевіряння ЕЦП національного проекту є аналогом відомої схеми цифрового підпису KCDSA, яка реалізована не з використанням перетворень у полі Галуа, а на еліптичних кривих. Схема, як і інші, розглянуті вище, є прикладом механізму вироблення цифрового підпису з додатком.

Параметри домену та параметри користувачів

Основними вимогами до параметрів домену та параметрів користувачів є такі:

– бітова довжина модуля n повинна бути більшою, ніж бітова довжина вихідного значення геш-функції $h()$;

– особистий і відкритий ключі об'єкта A, d_A і P_A відповідно необхідно виробляти згідно з процедурою, визначеною в стандарті ISO/IEC 15946-1 [30–32];

– об'єкт A повинен використовувати геш-значення z_A, що одержується відображенням даних відкритого сертифіката *Cert_Data* , які є відкритою інформацією. У цьому стандарті *Cert_Data* позначає дані сертифіката об'єкта A, які містять щонайменше розпізнавальний ідентифікатор об'єкта A, відкритий ключ P_A і всі параметри домену.

Допускаючи, що сертифікат включає все з описаного вище, більшість безпосередніх реалізацій для *Cert_Data* повинні бути самими сертифікатами.

Процес вироблення цифрового підпису

Вхідними даними для процесу цифрового підпису є такі:

– справжні та дійсні параметри домену;

– особистий ключ d_A підписувача;

– геш-значення z_A, одержане відображенням даних сертифіката *Cert_Data* підписувача;

– повідомлення M, яке належить підписати.

Вихідними даними за результатом вироблення цифрового підпису є пара (r, s), яка становить цифровий підпис повідомлення M об'єкта A. Перша частина підпису r є геш-значенням, а друга частина s є позитивним цілим числом, меншим за n.

При підписуванні повідомлення M об'єктом A виконуються такі кроки:

1) обчислюється геш-значення $e = h(z_A \mid M)$;

2) вибирається або генерується випадкове ціле число k, що належить діапазону $\{1, ..., n-1\}$;

3) обчислюється значення точки еліптичної кривої $(x_1, y_1) = kG$;

4) значення координати x_1 перетворюється на байтовий рядок і присвоюється змінній c;

5) обчислення геш-значення $r = h(kG) = h(c)$, яке і є відкритим ключем сеансу.

У рівнянні $r = h(kG) = h(c)$ припускається, що $h(kG)$ – це функція, що виділяє x – координату точки kG, перетворює її на байтовий рядок, а потім перетворює одержане значення за допомогою певної геш-функції $h()$ на ключ сеансу.

Крім того, оскільки обчислене значення r не залежить від підписуваного повідомлення, число r може обчислюватися попередньо, і надалі зберігатися та використовуватися під час вироблення цифрового підпису.

6) обчислюється значення $w = r \; XOR \; e$. Якщо $w \geq n$, тоді $w = w - n$.

7) обчислюється безпосереднє значення цифрового підпису $s = d_A (k - w) \bmod n$.

Якщо в процесі вироблення цифрового підпису $s = 0$ або $r = 0$, то вироблення цифрового підпису необхідно повторити з новим випадковим значенням k.

Але, як зазначалося для інших цифрових підписів, імовірність того, що $r = 0$ або $s = 0$, є надзвичайно малою, якщо k обрано відповідно до вимог п. 2.

Таким чином, пара цілих чисел (r, s) становить цифровий підпис повідомлення M об'єкта A.

Перевіряння цифрового підпису

Перевіряння цифрового підпису виконується за 4 кроки:

1) перевіряння розміру цифрового підпису;

2) обчислення геш-значення повідомлення;

3) обчислення на еліптичних кривих;

4) перевіряння цифрового підпису.

Вхідними даними для процесу перевіряння цифрового підпису є такі:

– параметри домену;

– відкритий ключ P_A об'єкта A;

– геш-значення z_A одержане відображенням даних сертифіката $Cert\_Data$ об'єкта A;

– одержане повідомлення M';

– одержаний цифровий підпис повідомлення M, представлений двома цілими числами r' та s'.

Під час перевіряння цифрового підпису повідомлення M' об'єкта A об'єктом B виконуються такі кроки:

1) перевіряння того, що $0 < s' < n$ та $len_{r'} \le len_{h()}$. Якщо хоч одна з умов не виконується, то цифровий підпис відхиляється;

2) обчислюється геш-значення $e' = h(z_A \mid M')$;

3) обчислюється $w' = r' \; XOR \; e'$. Якщо $w' \ge n$, то $w' = w' - n$;

4) обчислюється значення точки еліптичної кривої $(x_1', y_1') = s'P_A + w'G$;

5) значення координати x_1' перетворюється на байтовий рядок та присвоюється змінній c;

6) обчислюється геш-значення $v = h(c)$.

Якщо $r' = v$, то цифровий підпис повинен прийматися перевірником. Якщо $r' \ne v$, тоді цифровий підпис повинен відхилятися перевірником.

Як і у випадку з відкритим ключем, якщо використовують несправжнє геш-значення z_A як вхідні дані, то процес перевіряння цифрового підпису буде автоматично невдалим.

2.4.5. Порівняння властивостей ЕЦП EC-DSA, EC-GDSA та EC-KCDSA

У цьому пункті наведено результати порівняння властивостей трьох алгоритмів цифрового підпису: EC-GDSA, EC-DSA та EC-KCDSA. У таблиці 2.6 наведено описи схем та їх особливості. У таблиці 2.7 наведено дані щодо оцінки складності обчислення та перевіряння цифрових підписів.

В алгоритмах EC-DSA та EC-GDSA використовується $h()\pi()$ функція для перетворення точки еліптичної кривої на ціле число, а в алгоритмі EC-KCDSA замість функції $\pi()$ використовується геш-функція $h()$. Складність обчислення значення геш-функції $h()$ перевершує складність обчислення функції перетворення $\pi()$. Однак частка обчислень геш-значень відносно загальних обчислень

є незначною. Окрім того, використання геш-функції в алгоритмі EC-KCDSA є засобом доведення стійкості. Більш того, при використанні двох функцій гешування в алгоритмі EC-KCDSA можна забезпечити стійкість за умови, якщо одна з функцій гешування є випадковим оракулом, а інша є колізійностійкою. На етапі вироблення цифрового підпису та при його перевірянні в алгоритмі EC-KCDSA не виконуються обчислення мультиплікативної інверсії за модулем n. Ці обчислення є достатньо складними в обмеженому обчислювальному середовищі, такому як старт-карти. Тому в деяких середовищах алгоритм EC-KCDSA може бути обчислювально більш ефективним, ніж EC-DSA. Алгоритм EC-GDSA забезпечує користувача покращеною процедурою підписування, при виконанні якої не використовуються обчислення мультиплікативної інверсії за модулем n, а також обчислення геш-функції для перетворення еліптичних кривих на цілі числа. Перевіряння цифрового підпису в EC-GDSA обчислювально еквівалентне перевіряню цифрового підпису в алгоритмі EC-DSA.

Алгоритм EC-DSA був схвалений (та рекомендований) федеральним урядом Сполучених Штатів, а уряд Південної Кореї запропонував до затвердження алгоритм EC-KCDSA.

Таблиця 2.6. **Порівняння описів та операцій**

	EC-DSA	**EC-GDSA**	**EC-KCDSA**
Таємні параметри безпеки	n, $h()$		
Вимоги до n	$n \geq 2^{\|h()\|}$	$n \geq 2^{\|h()\|}$	$n \geq 2^{\|h()\|-1}$
Особистий ключ	$d_A \in \{1, ..., n-1\}$		
Обчислення відкритого ключа	$P_A = d_A G$	$P_A = (d_A^{-1} \bmod n) G$	$P_A = (d_A^{-1} \bmod n) G$
Вироблення цифрового підпису	$k \in \{1, ..., n-1\}$ $r = \pi(kG) \bmod n$ $s = (d_A r + h(M)) k^{-1} \bmod n$	$k \in \{1, ..., n-1\}$ $r = \pi(kG) \bmod n$ $s = (kr - h(M)) d_A \bmod n$	$k \in \{1, ..., n-1\}$ $r = h(kG)$ $s = d_A(k - r \, XOR \, h(z_A \| M)) \bmod n$
Розмір цифрового підпису	$0 < r < n$, $0 < s < n$	$0 < r < n$, $0 < s < n$	$0 < s < n$, $0 \leq r < 2^{\|h()\|}$
Перевіряння цифрового підпису	$u_1 = s'^{-1} h(M') \bmod n$ $u_2 = s'^{-1} r' \bmod n$ $\pi(u_1 G + u_2 P_A) \bmod n = r'$?	$u_1 = r'^{-1} h(M') \bmod n$ $u_2 = r'^{-1} s' \bmod n$ $\pi(u_1 G) + u_2 P_A \bmod n = r'$?	$e = r' \, XOR \, h(z_A \| M') \bmod n$ $h(s' P_A) + e' G = r'$?

Таблиця 2.7. **Порівняння числа операцій ЕЦП EC-DSA, EC-GDSA та EC-KCDSA**

Процес	Операція	EC-DSA	EC-GDSA	EC-KCDSA
Вироблення цифрового підпису	$h()$	1	1	2
	$\pi()$	1	1	0
	$k^{-1} \bmod n$	1	0	0
	Множення в Z_n	2	2	1
	Додавання (або віднімання) в Z_n	1	1	1
	Скалярне множення точки кривої	1	1	1
Перевіряння цифрового підпису	$h()$	1	1	2
	$\pi()$	1	1	0
	s^{-1} (або r^{-1}) $\bmod n$	1	1	0
	Множення в Z_n	2	2	0
	Скалярне множення точки кривої	2	2	2
	Додавання точок на кривій	1	1	1

2.5. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ЗГІДНО З ДСТУ 4145-2002

Національний стандарт ДСТУ 4145-2002 [35] визначає механізм електронного цифрового підпису, що ґрунтується, як і розглянуті вище ЕЦП згідно з ISO/IEC 14888-3 (15946-2), на властивостях груп точок еліптичних кривих над полями $GF(2^m)$. Цифровий підпис забезпечує автентичність повідомлення та неспростовність застосування особистого ключа, тобто автентифікацію власника цифрового підпису. При його застосуванні з необхідною ймовірністю гарантується цілісність підписаного повідомлення, автентичність його автора та неспростовність підписаного документа. У стандарті для генерування випадкових послідовностей використовуються міждержавний стандарт ГОСТ 28147-89 та ГОСТ 34.311-94 для обчислення геш-функції підписуваного повідомлення; детальний повний опис стандарту міститься в [41].

У стандарті для отримання випадкових даних, необхідних для побудови загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифровою підпису використовується генератор псевдовипадкових послідовностей. По суті, він ґрунтується на стандарті

ANSI США X 9.17 [172]. Допускається використання будь-якого іншого генератора, рекомендованого уповноваженим виконавчим органом державної влади.

Обов'язковою складовою ЕЦП національного стандарту є функція гешування H. Вона, як і в інших стандартах, застосовується в процесі обчислення й перевірки цифрового підпису.

Функція гешування H перетворює інформацію M довільної довжини L_T на двійковий рядок $H(M)$ фіксованої довжини L_H. Повинна використовуватися функція гешування, визначена в ГОСТ 34.311-95, або будь-яка інша функція гешування, рекомендована уповноваженим виконавчим органом державної влади. Значення параметра довжини геш-значення L_H однозначно визначається ідентифікатором iH конкретної функції гешування, що використовується сумісно з національним стандартом ЕЦП, він належить до загальних параметрів ЕЦП. Значення $iH = 1$, $L(iH) = 8$ відповідають функції гешування, що визначена в ГОСТ 34.311-95.

2.5.1. Обчислення та використання загальних параметрів ЕЦП

Загальні параметри цифрового підпису можуть бути однаковими для довільного числа користувачів цифрового підпису. Наведемо правила обчислення загальних параметрів цифрового підпису.

При обчисленні ЕЦП дозволяється використовувати як основне поле з поліноміальним або оптимальним нормальним базисом. За умови, що використовується поліноміальний базис, основне поле треба вибирати серед полів $GF(2^m)$, степені яких наведено в таблиці 2.8. Тобто поліноміальний базис задають незвідним (примітивним) тричленом або незвідним п'ятичленом. Згідно зі стандартом використання незвідних многочленів, наведених у таблиці 2.8, не є обов'язковим [35].

Таблиця 2.8. **Допустимі основні поля з поліноміальним базисом і рекомендовані незвідні многочлени**

№ з/п	Степінь поля m	Примітивний многочлен	№ з/п	Степінь поля m	Примітивний многочлен
1	2	3	4	5	6
1	163	$x^{163}+x^7+x^6+x^3+1$	31	337	$x^{337}+x^{10}+x^6+x+1$
2	167	$x^{167}+x^6+1$	32	347	$x^{347}+x^{17}+x^6+x+1$
3	173	$x^{173}+x^{10}+x^2+x+1$	33	349	$x^{349}+x^6+x^5+x^2+1$
4	179	$x^{179}+x^4+x^2+x+1$	34	353	$x^{353}+x^{26}+x^7+x^3+1$
5	181	$x^{181}+x^7+x^6+x+1$	35	359	$x^{359}+x^{18}+x^4+x^2+1$
6	191	$x^{191}+x^9+1$	36	367	$x^{367}+x^{21}+1$
7	193	$x^{193}+x^{15}+1$	37	373	$x^{373}+x^9+x^6+x+1$

Закінчення табл. 2.8

1	2	3	4	5	6
8	197	$x^{197}+x^{21}+x^2+x+1$	38	379	$x^{379}+x^{17}+x^6+x+1$
9	199	$x^{199}+x^{11}+x^2+x+1$	39	383	$x^{383}+x^9+x^5+x+1$
10	211	$x^{211}+x^{12}+x^6+x+1$	40	389	$x^{389}+x^{17}+x^{10}+x+1$
11	223	$x^{223}+x^{12}+x^2+x+1$	41	397	$x^{397}+x^{22}+x^3+x+1$
12	227	$x^{227}+x^{21}+x^2+x+1$	42	401	$x^{401}+x^{29}+x^4+x+1$
13	229	$x^{229}+x^{21}+x^2+x+1$	43	409	$x^{409}+x^{15}+x^6+x+1$
14	233	$x^{233}+x^9+x^4+x+1$	44	419	$x^{419}+x^{21}+x^{14}+x+1$
15	239	$x^{239}+x^{15}+x^2+x+1$	45	421	$x^{421}+x^7+x^4+x+1$
16	241	$x^{241}+x^{15}+x^4+x+1$	46	431	$x^{431}+x^5+x^3+x+1$
17	251	$x^{251}+x^{14}+x^4+x+1$	47	433	$x^{433}+x^{15}+x^5+x+1$
18	257	$x^{257}+x^{12}+1$	48	439	$x^{439}+x^8+x^3+x^2+1$
19	263	$x^{263}+x^{27}+x^2+x+1$	49	443	$x^{443}+x^{28}+x^3+x+1$
20	269	$x^{269}+x^7+x^6+x+1$	50	449	$x^{449}+x^{25}+x^5+x^3+1$
21	271	$x^{271}+x^{16}+x^3+x+1$	51	457	$x^{457}+x^{16}+1$
22	277	$x^{277}+x^{23}+x^3+x^2+1$	52	461	$x^{461}+x^{23}+x^4+x+1$
23	281	$x^{281}+x^9+x^4+x+1$	53	463	$x^{463}+x^{24}+x^3+x+1$
24	283	$x^{283}+x^{26}+x^9+x+1$	54	467	$x^{467}+x^{28}+x^3+x+1$
25	293	$x^{293}+x^{11}+x^6+x+1$	55	479	$x^{479}+x^{25}+x^6+x+1$
26	307	$x^{307}+x^8+x^4+x^2+1$	56	487	$x^{487}+x^{15}+x^2+x+1$
27	311	$x^{311}+x^{29}+x^4+x+1$	57	491	$x^{491}+x^{17}+x^6+x^2+1$
28	313	$x^{313}+x^7+x^3+x+1$	58	499	$x^{499}+x^{29}+x^6+x^2+1$
29	317	$x^{317}+x^9+x^5+x^2+1$	59	503	$x^{503}+x^3+1$
30	331	$x^{331}+x^{12}+x^5+x^2+1$	60	509	$x^{509}+x^{23}+x^3+x^2+1$

Незвідні поліноми степенів включно до 2000 степеня можна знайти в X 9.62 [44] та X 9.63 [52].

Якщо використовують оптимальний нормальний базис, то основне поле слід вибирати серед полів $GF(2^m)$, степені яких наведено в таблиці 2.9.

Таблиця 2.9. **Допустимі основні поля з оптимальним нормальним базисом**

Степінь поля m	173	179	191	233	239	251	281
Степінь поля m	293	359	419	431	443	491	509

Національний стандарт регламентує використання еліптичних кривих. Так, для будь-якого з наведених у таблицях 2.8 та 2.9 основних полів і порядки базової точки, що їм відповідають, надаються у встановленому порядку уповноваженим виконавчим органом державної влади. Дозволено використовувати еліптичні криві, що наведені в додатку Г національного стандарту.

Національний стандарт також встановлює алгоритм обчислення базової точки еліптичної кривої над основним полем. Його сутність полягає в такому.

Вхідні дані алгоритму: параметри (коефіцієнти) еліптична кривої A, B і порядок базової точки n повинні прийматися згідно із зазначеним вище.

Результат виконання алгоритму – базова точка еліптичної кривої P.

Алгоритм обчислення базової точки

1. Обчислюється випадкова точка P згідно з п. 6.8 стандарту.
2. Обчислюється точка еліптичної кривої $R = nP$.
3. Якщо $R \neq 0$, то переходимо до кроку 1, інакше – до кроку 4.
4. Результат виконання алгоритму – базова точка P еліптичної кривої.

Базова точка задається її координатами в афінному чи проективному базисах. Допускається зберігання та передача базової точки у стисненому вигляді згідно з вимогами стандарту. За необхідності відновлення базової точки виконують згідно з п. 6.10 стандарту.

2.5.2. Перевірка правильності загальних параметрів ЕЦП

Задекларований рівень криптографічної стійкості ЕЦП, що встановлено цим стандартом, гарантується за умови, якщо загальні параметри цифрового підпису обчислені строго відповідно до національного стандарту.

Обов'язковими є такі перевірки:

1) перевірка правильності вибору основного поля;

2) перевірка правильності вибору рівняння еліптичної кривої та порядку базової точки;

3) перевірка правильності базової точки.

Перевірка правильності вибору основного поля

Якщо основне поле задане поліноміальним базисом, то перевіряється виконання таких умов:

1) степінь основного поля міститься в таблиці 2.8;

2) основне поле задано незвідним тричленом або незвідним п'ятичленом;

3) перевірку незвідності многочлена виконують згідно з п. 6.11 стандарту тільки за умови, що незвідний многочлен не міститься в таблиці 2.8.

Якщо основне поле задане оптимальним нормальним базисом, то перевіряється наявність степеня основного поля в таблиці 2.9.

Якщо умови 1–3 виконано, то основне поле обрано правильно. Указану перевірку можна не виконувати, якщо виконання умов гарантується іншим чином.

Перевірка правильності вибору рівняння еліптичної кривої

Перевірка правильності вибору коефіцієнтів (A, B) рівняння еліптичної кривої:

1) коефіцієнт k належить основному полю, тобто є двійковим рядком довжини m;

2) коефіцієнт A дорівнює 0 або 1;

3) коефіцієнт $B \neq 0$.

Перевірка правильності порядку n базової точки еліптичної кривої

1) n – просте непарне число, простота перевіряється згідно з п. 6.12 стандарту;

2) $n \geq \max\left(2^{160}, 4\left(\left\lfloor\sqrt{2^m}\right\rfloor + 1\right)\right)$;

3) $2^{mk} \neq 1 \bmod n$ для $k = 1, \ldots, 32$ (умова Менезеса – Окамото – Венстона). Ця умова перевіряється згідно з п. 6.13 стандарту.

Якщо умови 1–6 виконано, то рівняння еліптичної кривої та порядок базової точки обрано правильно. Указані перевірки можна не виконувати, якщо використані в конкретній реалізації способи отримання й зберігання коефіцієнтів рівняння еліптичної кривої та порядку базової точки цієї кривої гарантують виконання зазначених умов.

Перевірка правильності базової точки

Базова точка $P = (x_p, y_p)$ еліптичної кривої повинна задовольняти таким умовам:

1) координати базової точки $P = (x_p, y_p)$ належать основному полю, тобто є двійковими рядками довжини;

2) $P \neq O$;

3) точка $P = (x_p, y_p)$ лежить на еліптичній кривій, тобто її координати задовольняють рівнянню вибраної еліптичної кривої;

4) $nP = O$.

Якщо умови 1–4 виконано, то базова точка еліптичної кривої правильна.

Зазначену перевірку можна не виконувати, якщо використані в конкретній реалізації способи обчислення й зберігання базової точки гарантують виконання умов 1–4.

2.5.3. Порядок обчислення ключів ЕЦП

Розглянемо порядок обчислення асиметричної пари ключів (d, Q), тобто особистого d і відкритого Q ключів цифрового підпису.

Обчислення особистого ключа цифрового підпису

Особистий ключ d цифрового підпису повинен генеруватись (обчислюватись) таким чином:

1) обчислюється випадкове ціле число d згідно з п. 6.3 стандарту;

2) перевіряється умова $d \neq 0$. Якщо вона виконується, то d обирають як особистий ключ цифрового підпису, інакше переходимо до кроку 1.

Необхідно відзначити, що недопустимим є використання особистого ключа $d = 1$ та $d = n - 1$, оскільки в цьому випадку відкритий ключ Q співпаде з базовою точкою G, що повністю компрометує такий особистий ключ.

Умови обчислення й зберігання особистого ключа цифрового підпису повинні унеможливлювати несанкціонований доступ до нього або його частини, а також до проміжних даних, які використовувалися в процесі обчислення особистого ключа. Окрім того, умови зберігання та використання особистого ключа повинні унеможливлювати його модифікацію, знищення або підміну. Цього можна досягти, використовуючи апаратні засоби зберігання та використання особистих ключів.

Обчислення відкритого ключа цифрового підпису

Відкритий ключ цифрового підпису обчислюється у вигляді точки з використанням скалярного множення вигляду $Q = -dP$, де P – як і раніше, базова точка. Використання від'ємного знаку пов'язане з прискоренням за таких умов обчислення цифрового підпису.

Щодо відкритого ключа мають бути забезпечені послуги його цілісності, справжності та доступності, у цьому забезпечується практична захищеність від модифікації, підміни та викривлення відкритого ключа цифрового підпису. Основним способом забезпечення таких властивостей є використання послуг третьої довірчої сторони, для національних систем – це використання послуг акредитованих центрів сертифікації ключів, тобто виготовлення та обслуговування сертифікатів відкритих ключів.

2.5.4. Перевірка правильності ключів ЕЦП

Необхідний рівень криптографічної стійкості ЕЦП від різних загроз і атак може бути забезпечений за умови забезпечення цілісності, справжності та доступності до асиметричної пари ключів (d, Q). Указане забезпечується постійною перевіркою правильності відкритого й особистого ключів цифрового підпису.

Перевірка правильності відкритою ключа ЕЦП

Відкритий ключ Q цифрового підпису, як правило, повинен використовуватись у вигляді сертифікату відкритого ключа та задовольняти таким умовам:

1) координати точки еліптичної кривої, що визначають відкритий ключ цифрового підпису, належать основному полю, тобто є двійковими рядками довжини m;

2) відкритий ключ задовольняє умові $Q \neq 0$ (він також має задовольняти умові $Q \neq P$, тобто $d = 1$);

3) відкритий ключ $Q = (x_Q, y_Q)$ задовольняє рівнянню використовуваної еліптичної кривої;

4) порядок точки n такий, що $nQ = 0$.

Якщо умови 1–4 виконані, то відкритий ключ цифрового підпису правильний.

Указану перевірку на практиці можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування засоби зберігання та використання відкритого ключа цифрового підпису унеможливлюють його підміну, модифікацію чи знищення.

Перевірка правильності особистого ключа

Перевірка правильності особистого ключа виконується тільки власником особистого ключа. Вона повинна здійснюватися таким чином:

1) обчислюється точка еліптичної кривої $Q' = -dP$, причому P – базова точка еліптичної кривої а d – особистий ключ цифрового підпису.

2) якщо $Q' = Q$, де Q – відкритий ключ цифрового підпису, то особистий ключ відповідає відкритому ключу цифрового підпису і є правильним.

Зазначену перевірку можна не виконувати, якщо використані в конкретній реалізації алгоритму ЕЦП засоби зберігання та використання особистого ключа практично виключають його підміну, модифікацію чи знищення.

2.5.5. Порядок обчислення цифрового передпідпису

Оскільки в стандарті особистий (таємний) ключ сеансу не залежить від повідомлення (інформації), що підписується, то попередньо він може бути обчислений та зберігатися в захищеному вигляді. У національному стандарті визначено такий механізм обчислення цифрового передпідпису.

Вхідними даними для формування цифрового передпідпису є загальні параметри.

Результатом виконання алгоритму є цифровий передпідпис F_e, що відповідає таємному випадковому параметру e, де e – ціле число, $0 < e < n$, $F_e \in GF(2^m)$, а n – порядок базової точки. (Зазвичай для інших ЕЦП особисте значення e позначалося літерою k. Але, зважаючи на позначення в стандарті, ми використовуємо символ e).

Алгоритм обчислення цифрового передпідпису

1. Обчислюється випадкове ціле число e згідно з п. 6.3 стандарту.

2. Обчислюється точка еліптичної кривої $R = e\,P = (x_R, y_R)$.

3. Якщо координата $x_R = 0$, то перейти до кроку 1, інакше $F_e = x_R$ і необхідно перейти до кроку 4.

4. Результат виконання алгоритму – цифровий передпідпис F_e та таємний випадковий параметр e.

Необхідно зауважити, що умови обчислення, зберігання й використання таємного параметра e мають унеможливлювати несанкціонований доступ до нього, його частин, а також до проміжних даних, які використовувалися в процесі обчислення цифрового передпідпису.

Припускається попереднє обчислення необхідного числа цифрових передпідписів, але за умови унеможливлення його модифікації чи підміни, а також обов'язкового знищення разом з відповідним таємним параметром e.

2.5.6. Порядок обчислення ЕЦП

Обчислення ЕЦП повинне виконуватися в такому порядку.

Задані та є доступними такі вхідні дані:

– загальні параметри цифрового підпису;

– особистий ключ цифрового підпису d;

– повідомлення T довжини $L_T > 0$;

– функція гешування H згідно з п. 6.2 стандарту;

– довжина цифрового підпису L_D, що вибирається для групи користувачів, виходячи з умов конкретної реалізації алгоритму цифрового підпису з урахуванням умов кроку 3 наведеного нижче алгоритму.

Результат виконання алгоритму: повідомлення T і цифровий підпис D, що дають змогу утворити підписане повідомлення у вигляді (iH, T, D).

Алгоритм цифрового підписування

1. Перевіряється правильність загальних параметрів цифрового підпису згідно з п. 8.1–8.3 стандарту. Якщо загальні параметри цифрового підпису обчислено неправильно, то обчислення цифрового підпису припиняється.

2. Перевіряється правильність особистого ключа цифрового підпису згідно з п. 10.2 стандарту. Якщо особистий ключ неправильний, то обчислення цифрового підпису припиняють.

3. Перевіряється виконання умов: L_D – число, кратне 16; $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконується, то обчислення цифрового підпису припиняється.

4. Якщо використовується ідентифікатор геш-функції iH, то перевіряється, чи діє цей ідентифікатор у відповідній групі користувачів. Якщо ні, то обчислення цифрового підпису припиняється.

5. Якщо нормативні документи, що визначають порядок обчислення функції гешування, накладають обмеження на довжину повідомлення L_T, то перевіряють виконання цих обмежень. Якщо ці обмеження не виконані, або повідомлення відсутнє, або $L_T \leq 0$, то обчислення цифрового підпису припиняється.

6. Для повідомлення T обчислюється геш-значення $h = H(T)$.

7. Результат обчислення функції гешування $H(T)$ перетворюють на елемент основного поля h згідно з п. 5.9 стандарту. Якщо $h = 0$, то приймають $h = 1$.

8. Якщо вже існує набір цифрових передпідписів, обчислених заздалегідь, то береться будь-який із них разом з відповідним таємним параметром. Інакше цифровий передпідпис обчислюється в спосіб, указаний вище в п. 2.5.5.

9. Обчислюється елемент основного поля $y = hF_e$.

10. Елемент основного поля y перетворюють на ціле число r згідно з п. 5.8 стандарту.

11. Якщо $r = 0$, то перейти до кроку 8; інакше перейти до кроку 12.

12. Обчислюється значення підпису у вигляді цілого числа $s = (e + dr) \bmod n$.

13. Якщо $s = 0$, то перейти до кроку 8; інакше перейти до кроку 14.

14. Пару цілих чисел (r, s) перетворюють на цифровий підпис D довжини L_D згідно з п. 5.10 стандарту.

15. Результат виконання алгоритму – підписане повідомлення (iH, T, D).

2.5.7. Порядок перевіряння ЕЦП

Перевіряння ЕЦП виконується в такому порядку.

Заданими та доступними є такі вхідні дані:

– загальні параметри цифрового підпису;

– відкритий ключ цифрового підпису підписувача Q;

– підписане повідомлення (iH, T, D) довжиною $L = L(iH) + L_T + L_D$;

– функція гешування H згідно з п. 6.2 стандарту.

Результатом виконання алгоритму є повідомлення «підпис дійсний» або «підпис не дійсний».

Алгоритм перевіряння цифрового підпису

1. Якщо використовується ідентифікатор геш-функції iH, то перевіряється, чи діє цей ідентифікатор у відповідній групі користувачів. Якщо ні, то видається повідомлення «підпис не дійсний» і припиняється перевіряння ЕЦП.

2. Виходячи з iH (або за мовчанням), визначають L_H.

3. Перевіряється виконання умов, що L_D – число, кратне 16 та $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконується, то видається повідомлення «підпис не дійсний» і перевірку припиняють.

4. Перевіряють правильність обчислення загальних параметрів цифрового підпису згідно з пп. 8.1–8.3 стандарту. Якщо загальні параметри цифрового підпису обчислено неправильно, то видається повідомлення «підпис не дійсний» і перевірку припиняють.

5. Згідно з п. 10.1 перевіряється правильність відкритого ключа ЕЦП. Якщо відкритий ключ обчислено неправильно, то видають повідомлення «підпис не дійсний» і перевірку припиняють.

6. Обчислюється $L_T = L - L_D - L(iH)$. У разі відсутності тексту, або при $L_T \leq 0$ видається повідомлення «підпис недійсний» і перевірку припиняють. Якщо нормативні документи, які встановлюють обчислення функції гешування, накладають обмеження на довжину повідомлення L_T, то перевіряють виконання цих умов. Якщо ці умови не виконані, то видають повідомлення «підпис недійсний» і перевірку підпису припиняють.

7. Для повідомлення T обчислюється геш-значення $h = H(T)$.

Геш-значення $H(T)$ перетворюється на елемент основного поля h згідно з п. 5.9 стандарту. Якщо $h = 0$, то приймається $h = 1$.

8. Згідно з п. 5.11 стандарту цифровий підпис D перетворюється на пару цілих чисел (r, s). Якщо умова $0 < r < n$ не виконана, то видається повідомлення «підпис недійсний» і перевірка припиняється.

9. Якщо умова $0 < s < n$ не виконана, то видається повідомлення «підпис недійсний» і перевірка припиняється.

10. Обчислюється точка еліптичної кривої $R = sP + rQ$, $R = (x_R, y_R)$.

11. Обчислюється елемент основного поля $y = hx_R$.

12. Елемент основного поля y перетворюють на ціле число $\tilde{r}$ згідно з п. 5.8 стандарту.

13. Перевіряється умова $r = \tilde{r}$; якщо вона виконується, то видається повідомлення «підпис дійсний», інакше видають повідомлення «підпис недійсний».

Доведемо, що обчислення ЕЦП з використанням виразу $s = (e + dr) \bmod n$ та перевірка згідно п. 10.1 з використанням

$$R = sP + rQ, \quad R = (x_R, y_R) \tag{2.14}$$

є правильним. Для цього зробимо такі перетворення. Помножимо ліві та праві частини (2.14) на базову точку P. У результаті маємо:

$$sP = eP + r\,Q. \tag{2.15}$$

За умови, що $R = eP = (x_R, y_R)$, з (2.15) маємо:

$$R = sP - rQ.$$

2.5.8. Порівняння складності виконання ЕЦП національних та міжнародних стандартів

У цьому пункті наведені результати порівняння складності виконання п'яти основних стандартів ЕЦП – ДСТУ 4145-2002, ГОСТ 34.10-2001, EC-GDSA, ECDSA та EC-KCDSA. У таблиці 2.10 наведено дані щодо оцінки видів та числа операцій, які повинні виконуватись при обчисленні та перевірці зазначених електронних цифрових підписів. Дані таблиці 2.10 отримані в результаті прямого аналізу алгоритмів обчислення та перевірки ЕЦП указаних стандартів.

Як випливає із даних таблиці 2.7, в алгоритмах ECDSA та EC-GDSA використовується $\pi()$ функція для перетворення точки еліптичної кривої на ціле число, а в алгоритмі EC-KCDSA замість функції $\pi()$ використовується геш-функція $h()$. Складність обчислення значення геш-функції $h()$ перевершує складність обчислення функції перетворення $\pi()$. Однак частка обчислень геш-значень відносно загальних обчислень є незначною. Крім того, використання геш-функції в алгоритмі EC-KCDSA є способом доведення стійкості. Більш того, при використанні двох функцій гешування в алгоритмі EC-KCDSA можна забезпечити стійкість за умови, якщо одна з функції гешування є випадковим оракулом, а інша є колізійно стійкою. На етапі вироблення цифрового підпису та при його перевірянні в алгоритмі EC-KCDSA не виконуються обчислення мультиплікативної інверсії за модулем n. Ці обчислення є достатньо складними в обмеженому обчислювальному середовищі, такому як старт-карти. Тому в деяких середовищах алгоритм EC-KCDSA може бути обчислювально більш ефективним, ніж ECDSA. Алгоритм EC-GDSA забезпечує користувача покращеною процедурою підписування, при виконанні якої не використовуються обчислення мультиплікативної інверсії за модулем n, а також обчислення геш-функції для перетворення еліптичних кривих на цілі числа. Перевіряння цифрового підпису в EC-GDSA обчислювально еквівалентне перевірянню цифрового підпису в алгоритмі ECDSA.

Алгоритм ECDSA був схвалений (та рекомендований) федеральним урядом Сполучених Штатів, а уряд Південної Кореї запропонував до затвердження алгоритм EC-KCDSA.

У таблиці 2.10 наведено значення складності обчислення ЕЦП та перевіряння ЕЦП для 5-ти основних ЕЦП, що реалізовані в групі точок еліптичних кривих – ECDSA, EC-GDSA, EC-KCDSA, ДСТУ 4145-2002 та ГОСТ Р 34.10-2001.

Як видно з таблиці, при обчисленні підпису для EC-KCDSA необхідно обчислити два значення функції гешування, а для інших – тільки одне значення. У той же час для EC-KCDSA не потрібно обчислювати значення $\pi()$ функції. Алгоритми ECDSA та ГОСТ Р 34.10-2001 потребують ділення за модулем, що є однією з найбільш складних операцій. Для EC KCDSA також необхідно виконувати одну операцію додавання в полі, у той час як для всіх інших необхідно виконати дві операції додавання в полі. У цілому, оскільки найбільш складною є операція ділення за модулем в полі, то алгоритми ECDSA та ГОСТ Р 34.10-2001, у порівнянні з іншими, є більш складними.

Відносно порівняння складності перевіряння ЕЦП за даними таблиці можна зробити такі висновки. В EC-KCDSA необхідно виконати обчислення двох значень функції гешування, у той час як для інших – одне обчислення. Суттєвим недоліком

ECDSA, EC-GDSA та ГОСТ 34.10-2001 є необхідність виконання операції ділення за модулем і знаходження $\pi()$ функції, а для інших виконувати цю операцію не потрібно. Для ECDSA, EC-GDSA та ГОСТ 34.10-2001 необхідно виконати дві операції множення за модулем у полі, для ДСТУ 4145-2002 – одну, а для EC-KCDSA – жодної. Окрім того, для стандартів, що розглядаються, необхідно виконувати перетворення з одного подання в інше. За необхідності більш точної оцінки рекомендується враховувати й ці операції згідно відповідних стандартів.

Таблиця 2.10. **Порівняння числа операцій ЕЦП для міжнародних та національних стандартів**

Процес	Операція	ECDSA	EC-GDSA	EC-KCDSA	ДСТУ 4145-2002	ГОСТ Р 34.10-2001
Вироблення цифрового підпису	$h()$	1	1	2	1	1
	$\pi()$	1	1	0	1	1
	$k^{-1} \bmod n$	1	0	0	0	1
	Множення в Z_n	2	2	1	2	2
	Додавання (або віднімання) в Z_n	1	1	1	1	1
	Скалярне множення точки кривої	1	1	1	1	1
Перевіряння цифрового підпису	$h()$	1	1	2	1	1
	$\pi()$	1	1	0	0	1
	s^{-1} (або r^{-1}) $\bmod n$	1	1	0	0	1
	Множення в Z_n	2	2	0	1	2
	Скалярне множення точки кривої	2	2	2	2	2
	Додавання точок на кривій	1	1	1	1	1