Розділ 1

ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ТА ЙОГО ЗАСТОСУВАННЯ

У XXI сторіччі у світовому інформаційному просторі та інформаційних просторах держав вирішуються складні завдання переходу до використання систем електронних документів та електронного документообігу, електронної торгівлі, електронних банківських систем, систем електронного документообігу, електронних баз даних тощо. Електронні системи знаходять широке впровадження в науці, освіті, управлінні державою тощо. Одночасно із зазначеним, у таких системах виникли суттєві протиріччя, пов'язані зі складністю надання в них користувачам і власникам послуг цілісності, справжності, доступності, неспростовності тощо [1–3, 7–14, 17–20, 51–53] з необхідним рівнем гарантій, які вимагають вирішення. Особливо актуальними ці проблеми стали з прийняттям у державах на міжнародному рівні, у тому числі в Україні, основоположних законів «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», «Про захист інформації в інформаційно-телекомунікаційних системах» [1–3], «Політики сертифікації ключів» тощо.

На виконання цих законів в Україні створюється інфраструктура відкритих ключів, перш за все для підтримки системи (електронного) цифрового підпису. При цьому першочерговим завданням в Україні, що вимагає свого вирішення, є надання органам державної влади, місцевого самоврядування, юридичним та фізичним особам послуг із забезпечення цілісності, справжності, неспростовності, а в більшості випадків і конфіденційності інформації та різноманітних даних, що представлені в електронному вигляді, електронних документів і повідомлень, програмного забезпечення, що ними використовуються. Крім того, у зв'язку з інтеграцією України у світовий інформаційний простір, орієнтацією на вступ України до Європейського співтовариства, важливим є завдання забезпечення взаємодії органів державної влади, місцевого самоврядування, юридичних і фізичних осіб на світовому рівні, з використанням іноземних і міжнародних інформаційних та інформаційно-комунікаційних систем, різноманітних інформаційних технологій, відкритих систем типу Інтернет тощо.

Практичний досвід і аналіз можливостей показують, що одним із основних і комплексних засобів забезпечення надання вказаних послуг є застосування (електронного) цифрового підпису (ЕЦП). На світовому рівні та в усіх технологічно розвинених державах якісне надання вказаних послуг, як правило, забезпечується

за рахунок застосування цифрового підпису та є кращою усталеною практикою. Для розв'язання цих завдань у технологічно розвинених державах створені інфраструктури відкритих ключів, прийняті та діють нормативно-правові акти, національні та міжнародні стандарти. Особлива увага на міжнародному рівні приділяється проблемам стандартизації. Прийняті та вже знайшли широке застосування базові стандарти на моделі та системи цифрового підпису ISO/IEC 9796-3 [29], ISO/IEC 14888-3 [34], ISO/IEC 15946-1, 2, 3, 4, 5 [15, 16, 27, 30, 33] та ISO/IEC 9594-8 | ITU-T Rec. X.509:2005 [13]. В Україні також уведено в дію та застосовується стандарт ЕЦП ДСТУ 4145-2002 [35], що реалізований на основі використання перетворень у групі точок еліптичних кривих, а також гармонізовані й діють стандарти ДСТУ ISO/IEC 15946-1, 3 та ДСТУ ITU-T Rec. X.509 | ISO/IEC 9594-8:2006 [14].

Обов'язковим реквізитом електронного документа є електронний підпис, або ЕЦП. Особливістю ЕЦП є те, що такий підпис отримується за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується. Застосування ЕЦП дає змогу підтвердити його цілісність, справжність і встановити авторство підписувача. Таким чином, починається широке застосування методів криптографії широким загалом користувачів, юридичних і фізичних осіб. Особливо проблематичним при застосуванні криптографічних перетворень є формування ключових даних і виготовлення ключових документів. По суті, для держави це складна проблема, яка вимагає розв'язання ряду задач законодавчого, організаційного, організаційно-технічного та програмно-технічного характеру. Результатом їхнього розв'язання є створення національної системи електронного цифрового підпису, що є за призначенням та можливостями аналогом міжнародної інфраструктури відкритих ключів.

У цьому розділі наводяться основні теоретичні і практичні результати щодо ЕЦП. Вони згруповані в такій послідовності: спочатку викладається матеріал основних положень в частині ЕЦП, що містить основні поняття й визначення, далі розглянуто класифікацію ЕЦП та вимоги до них.

1.1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

На наш погляд, як основні поняття криптології, що відображають новітні досягнення у сфері електронних документів та електронного документообігу в частині застосування ЕЦП, можуть бути прийняті й використовуватись такі [1–3, 5, 6, 7, 9, 13, 15, 29, 30]:

Електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

(Електронний) цифровий підпис (ЕЦП) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа

та перевіряється за допомогою відкритого ключа. Нижче обґрунтовується необхідність уточнення наведеного поняття ЕЦП.

Уточнення поняття цифрового підпису. Вважається, що необхідно зробити уточнення поняття ЕЦП. Уточнення пов'язане з визначенням ЕЦП. Оскільки сьогодні Україна орієнтується на європейський вибір, то, на наш погляд, при визначенні цифрового підпису треба зважати на Директиву 1999/93/ЄС. У той же час у вищевказаному визначенні цифрового підпису як ефект пропонується «...і дає змогу підтвердити його цілісність та автентифікувати підписувача». Уточнення пов'язане з тим, що замість терміну «ідентифікація» необхідно використовувати термін «автентифікація». Дійсно, поняття ідентифікації, як правило, міститься у присвоєнні та пред'явленні «...ідентифікатора. У той же час застосування ЕЦП забезпечує в тому числі перевіряння справжності (автентичності) підписувача, тобто ЕЦП забезпечує можливість перевірки цілісності та справжності даних, а також встановлення автентичності джерела повідомлення» [5]. Таким чином, застосування ЕЦП дозволяє насправді забезпечити три основні послуги – підтвердити цілісність і справжність (автентичність) інформації (даних, повідомлень, джерела тощо), а також спочатку ідентифікувати, а потім і перевірити (верифікувати) справжність (автентичність) підписувача.

Необхідно, на наш погляд, забезпечити сумісність національної термінології з Європейською. Аналіз показав, що поняття електронного цифрового підпису, що міститься в законі України «Про електронний цифровий підпис», відрізняється від закріпленого в Директиві 1999/93/ЄС. На підтвердження цього нижче наводимо витяги з Директиви 1999/93/ЄС Європейського парламенту і Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах співтовариства.

Стаття 2 (оригінал):

'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'.

Таким чином, як визначення ЕЦП пропонується таке.

(Електронний) цифровий підпис – сукупність даних, отриманих за результатом певного криптографічного перетворення деякого набору даних, яка додається до цього набору даних або логічно поєднується з ним і дає змогу підтвердити його цілісність і справжність і перевірити справжність (автентичність) підписувача».

Можливі й інші визначення. Так, у ISO/IEC 9796-1 [29] під ***(цифровим) підписом*** розуміють бітовий рядок, який є результатом процесу підписування.

В ISO/IEC 14888-3 [34] разом із поняттям підпису надається три взаємопов'язаних поняття – підпис, процес генерації підпису та процес верифікації підпису, що наводяться нижче.

(Цифровий) підпис – пара октетного рядка й цілого числа для забезпечення автентифікації, що обчислюються в процесі генерації підпису.

Процес генерації (цифрового) підпису – процес, що приймає як вхідні дані повідомлення, ключ підпису й загальні параметри, і видає як вихідні дані (цифровий) підпис.

Процес верифікації (цифрового) підпису – процес, який приймає як вхідні дані підписане повідомлення, ключ верифікації й загальні параметри області та видає як вихідні дані відновлене повідомлення, якщо вони (вхідні дані та повідомлення) справжні.

Додатково до визначень, наведених вище, також будемо використовувати такі.

Засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначений для генерації ключів, вироблення та (або) перевірки електронного цифрового підпису.

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр криптографічного алгоритму електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа.

Сертифікат відкритого ключа (далі сертифікат ключа) – документ, виданий центром сертифікації ключів, що засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі документа на папері та використовуватись для ідентифікації особи підписувача.

Посилений сертифікат відкритого ключа (далі посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам Закону «Про електронний цифровий підпис» від 22.05.03 № 825-IV, виданий акредитованим центром сертифікації ключів, засвідчувальним центром або центральним засвідчувальним органом.

Акредитація – процедура документального засвідчення компетенції центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів.

Компрометація особистого ключа – будь-яка подія та (або) дія, що призвела або може призвести до несанкціонованого використання особистого ключа.

Блокування сертифіката ключа – тимчасове призупинення чинності сертифіката ключа.

Підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа.

Послуги електронного цифрового підпису – надання користувачеві засобів електронного цифрового підпису, допомоги при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування й поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації й інші послуги, визначені Законом «Про електронний цифровий підпис» від 22.05.03 № 825-IV.

Надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний

висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється в порядку, визначеному законодавством.

Також необхідно відзначити, що існує декілька неофіційно розповсюджених визначень (електронного) цифрового підпису щодо документів. У найбільш узагальненому випадку під ЕЦП розуміють деякий числовий еквівалент звичайного підпису (штампу, печатки, водяного знаку тощо), наявність яких дозволяє встановити цілісність і достовірність документа. Підробити цей підпис можливо лише з імовірністю, що не перевищує допустиму, тобто ймовірність обману менше допустимої величини: $P_{обм} \leq P_{доп}$. Електронний цифровий підпис накладається за допомогою особистого ключа і перевіряється за допомогою відкритого ключа.

1.2. ОСОБЛИВОСТІ НАДАННЯ ПОСЛУГ БЕЗПЕКИ В ЕЛЕКТРОННОМУ ДОКУМЕНТООБІГУ

При здійснені електронного документообігу згідно з вимогами нормативно-правових актів повинні бути надані такі послуги, як цілісність, справжність і неспростовність інформації тощо. З точки зору складності, однією з найбільш складних послуг захисту електронних документів та електронного документообігу є послуга неспростовності. До основних послуг неспростовності належать: неспростовність джерела інформації; неспростовність доставки повідомлення; неспростовність подання інформації; неспростовність транспортування інформації (повідомлення).

Розглянемо спочатку основні поняття щодо послуг неспростовності.

Послуги неспростовності надають свідчення, з використанням якого встановлюється відповідальність суб'єкта чи об'єкта щодо конкретної дії або події [17–20]. Суб'єкт (об'єкт), який відповідає за дію або пов'язаний з подією, з використанням яких пов'язане вироблення свідчення, має назву *суб'єкт свідчення*. Основним типом свідчень, від яких залежить неспростовність, є застосування криптографічних перетворень типу ЕЦП та направленого шифрування (НШ).

З метою формування вичерпної інформації неспростовності для визначених засобів забезпечення неспростовності та середовища застосування цих засобів, залежно від діючої політики неспростовності, може використовуватися додаткова інформація та, наприклад:

– свідчення, яке містить довірчу позначку часу, що надається уповноваженим на фіксування часу;

– свідчення, що надається нотаріусом, який затверджує створення даних або дій чи подій, що здійснені одним чи більше суб'єктами (об'єктами).

Послуга неспростовності може надаватися лише для явно визначеної політики безпеки для конкретного засобу забезпечення неспростовності та середовища його використання.

Політика неспростовності – це сукупність правил (критеріїв) забезпечення надання послуг неспростовності. Тобто сукупність правил, які застосовуються для генерації та перевірки свідчень, а також для прийняття судових рішень.

З метою доведення неспростовності здійснюють обмін інформацією неспростовності. Він являє собою послідовність однієї чи більше передач інформації неспростовності з метою доведення неспростовності. Під ***інформацією неспростовності*** розуміють набір інформації, яка може містити інформацію щодо подій або дій, для яких генерувалися та були підтверджені свідчення, інформація щодо самих свідчень та діючої політики неспростовності.

Основними поняттями щодо послуг неспростовності є такі [17–20].

Неспростовність створення – послуга, призначена для унеможливлення відмови суб'єкта від факту створення та змісту повідомлення (тобто забезпечення відповідальності за зміст повідомлення та його створення).

Неспростовність доставки – послуга, призначена для унеможливлення відмови одержувача від факту одержання ним повідомлення та факту ознайомлення зі змістом повідомлення.

Неспростовність знання – послуга, призначена для унеможливлення відмови одержувача від факту ознайомлення зі змістом одержаного повідомлення.

Неспростовність джерела – послуга, призначена для унеможливлення відмови джерела від факту створення самого повідомлення та факту його надсилання.

Неспростовність одержання – послуга, призначена для унеможливлення відмови одержувача від факту одержання повідомлення.

Неспростовність відправлення – послуга, призначена для унеможливлення відмови відправника від факту надсилання повідомлення.

Неспростовність представлення – послуга, призначена для надання свідчення, що уповноважений на доставку прийняв повідомлення для передавання.

Неспростовність транспортування – послуга, призначена для надання свідчення для джерела повідомлення, що уповноважений на доставку доставив повідомлення до відповідного одержувача.

Основним засобом надання вказаних послуг є застосування асиметричних криптографічних перетворень типу ЕЦП та НШ. При виконанні обох перетворень застосовується пара ключів – особистий і відкритий.

1.3. АСИМЕТРИЧНІ КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ

У цілому криптографічні перетворення розподіляються на два великих класи [7–10, 51]:

1) *симетричні*, якщо виконується умова

$$K_j = K'_j \tag{1.1}$$

або один із ключів обчислюється за умови відомого другого не вище, ніж з поліноміальною складністю;

2) *асиметричні*, якщо виконується умова

$$K_j \neq K'_j \tag{1.2}$$

причому один із ключів може бути обчислений за умови відомого другого, не нижче, ніж із субекспоненційною складністю.

Основними ознаками для асиметричних криптоперетворень є види пар ключів та набори загальних чи загально системних параметрів. Кожне криптоперетворення задається прямим і зворотним перетворенням:

$$F_{\text{пр}}(M_i, K_j, Pr),$$
$$F_{\text{зв}}(M_i^3, K_j', Pr). \tag{1.3}$$

Основні асиметричні криптоперетворення, що застосовуються в системах електронного документообігу, ґрунтуються на використанні певного математичного апарату. Історично з'явилися й застосовуються криптографічні перетворення, що ґрунтуються на використанні математичного апарату:

– перетворення в кільці цілих чисел N_Z;
– перетворення в простих полях Галуа $F(q)$;
– перетворення в групі точок еліптичних кривих $E(F(q))$;
– перетворення на основі спарювання точок еліптичних кривих тощо.

1.3.1. Сутність асиметричних криптоперетворень у кільці цілих чисел

Розглянемо сутність перетворення на прикладі направленого шифрування [7–10, 46, 51, 64].

Нехай M_i – блок інформації, який треба захистити. Представимо цей блок у вигляді цілого числа з l_M бітами. Для виконання криптографічного перетворення в кільці (наприклад RSA) використовується ключова пара – два цілих числа (E_k, D_k), яка породжується випадково.

Пряме перетворення:

$$C_i = M_i^{E_k} (\text{mod}\, N), \tag{1.4}$$

причому ключова пара (E_k, D_k) зв'язана рівнянням

$$E_k \cdot D_k \equiv 1 (\text{mod}\, \varphi(N)), \tag{1.5}$$

причому $\varphi(N)$ – функція Ейлера.

$$\varphi(N) = \varphi(P \cdot Q) = (P-1)(Q-1), \tag{1.6}$$

а P та Q – великі прості числа спеціального вигляду.

Зворотне перетворення:

$$M_i \Rightarrow C_i^{D_k} (\text{mod}\, N) = M_i^{E_k D_k} (\text{mod}\, N) = M_i, \tag{1.7}$$

тобто перетворення зворотне й однозначне.

Залежно від криптографічного перетворення один із ключів оголошується особистим, другий – відкритим. Наприклад, для цифрового підпису E_k використовується як особистий ключ, а D_k як відкритий ключ. Для направленого шифрування як ключ зашифрування використовується відкритий ключ, а для розшифрування особистий ключ. Причому щодо особистих ключів мають бути забезпечені їхня конфіденційність, справжність, цілісність, доступність, спостережливість і неспростовність, а щодо відкритих ключів не обов'язково надавати тільки послугу конфіденційності. Також необхідно враховувати, що для НШ має використатись інша пара ключів, наприклад (E_j, D_j).

1.3.2. Сутність асиметричних криптоперетворень у полі Галуа

Розглянемо сутність асиметричних криптоперетворень у полі Галуа на прикладі направленого шифрування [7–10, 44, 40, 46, 64].

Нехай є просте поле Галуа $F(p)$. Для кожного p існує множина первісних елементів Θ_v розміру $\varphi(\varphi(p))$, де φ – функція Ейлера [7–9].

Кожний первісний елемент породжує поле:

$$\Theta_v^i \pmod p,\ i = \overline{0, p-1},$$

Криптоперетворення пов'язані з побудуванням пари ключів. Нехай є два користувачі A та B. Користувачі спочатку незалежно генерують випадково особисті ключі X_A, X_B довжиною l_k, а потім обчислюють відкриті ключі Y_A, Y_B, як це наведено нижче в таблиці 1.1.

Таблиця 1.1. **Генерування асиметричної пари ключів у полі Галуа**

A	B
X_A	X_B
$Y_A = \Theta_v^{X_A} \pmod p$	$Y_B = \Theta_v^{X_B} \pmod p$

При шифруванні використовуються властивості поля:

$$C_i = M_i \cdot Y_B^r \pmod p,$$
$$C_i' = \Theta_v^r \pmod p, \tag{1.8}$$

де r – ключ сеансу.

Користувач A передає користувачу B пару $\{C_i', C_i\}$. Потім користувач B направлене розшифровує з використанням свого особистого ключа X_B:

$$\frac{C_i}{(C_i')^{X_B}} = \frac{M_i \cdot Y_B^r \pmod p}{\Theta_v^{r \cdot X_B} \pmod p} = M_i. \tag{1.9}$$

Таким чином, перетворення в полі є зворотнім та однозначним.

Відзначимо, що задача криптоаналітика полягає в тому, щоб знайти особистий ключ розшифрування X_B. Розв'язуючи рівняння $Y_A = \Theta_v^{X_A} \pmod p$ відносно X_B, або рівняння $Y_B = \Theta_v^{X_B} \pmod p$, одержимо відповідно особистий (секретний) ключ X_A чи X_B. Стійкість проти атак у полі визначається складністю розв'язання рівняння відносно X_A чи X_B.

1.3.3. Сутність асиметричних криптоперетворень у групі точок еліптичних кривих

За останні 20 років розроблено нові математичні апарати, які дозволяють ефективно розв'язувати рівняння, що реалізовані в полях та кільцях. У 90-х роках було запропоновано використовувати криптоперетворення, що базуються

на перетвореннях у групі точок еліптичних кривих над полями $F(p)$, $F(2^m)$, $F(p^m)$ [44–52, 30–32, 7–10, 35, 46, 51, 64].

Основні положення та математичні методи криптографічних перетворень у групі точок еліптичних кривих наведено в додатку А.

Для випадку простого поля $F(p)$ рівняння має вигляд:

$$y^2 = x^3 + ax + b(\mathrm{mod}\, p). \tag{1.10}$$

Елементом перетворення є точка на еліптичній кривій, тобто (x_i, y_i), що обчислюється за модулем p. Ключова пара

$$(d_A, Q_A), \text{ де } 1 \le d_A < n$$

генерується випадково, причому d_A генерується випадково, а відкритий ключ обчислюється згідно з правилом

$$Q_A = d_A \cdot G(\mathrm{mod}\, p), \tag{1.11}$$

де G – базова точка на еліптичній кривій порядку n, а Q_A – відкритий ключ, точка на еліптичній кривій (ЕК) з координатами (x_a, y_a).

Параметри кривої a та b мають задовольняти умові:

$$4a^3 + 27b^2 \neq 0(\mathrm{mod}\, p). \tag{1.12}$$

Точка (x_i, y_i) належить ЕК, якщо ця пара чисел задовольняє рівнянню (1.10).

Над розширеним полем $GF(2^M)$ рівняння ЕК має вигляд:

$$y^2 + xy \equiv (x^3 + ax^2 + b)(\mathrm{mod}\, f(x), 2), \tag{1.13}$$

де (x_i, y_i) – точка ЕК; a, b – коефіцієнти (параметри) ЕК; $f(x)$ – незведений поліном над полем $GF(2)$.

Поліном називається *незведеним*, якщо він є таким, що не зводиться, а з іншого боку породжує поле періоду $2^m - 1$.

Існує тривимірне подання ЕК, що називається проективною геометрією (базисом). У проективній геометрії кожна точка задається трьома координатами – X, Y, Z.

Основною операцією в групі точок ЕК є скалярне множення вигляду (1.11) для простого поля $F(p)$, а для розширення $F(2^m)$:

$$Q = d \cdot G(\mathrm{mod}\, F(x), 2). \tag{1.14}$$

Стійкість атаки проти загрози повного розкриття визначається складністю розв'язання рівнянь (1.11) і (1.14) відносно особистого ключа d. Складність розв'язування цього рівняння набагато вища, ніж у кільці та полі. У полі – субекспоненційна, а в групі точок еліптичних кривих – експонентна складність.

1.3.4. Перетворення зі спарюванням точок еліптичних кривих

При викладенні сутності та можливостей ЕЦП будемо дотримуватись термінології, визначення та основних положень, визнаних відносно ЕЦП в ІВК із сертифікатами ключів.

Розглянемо чотири основних етапи реалізації ЕЦП на ідентифікаторах – генерування загальних параметрів, генерування ключів, вироблення та перевіряння ЕЦП на прикладі SOK-IBS системи.

До загальних параметрів будемо відносити адитивну групу G_1, що задається стандартно відповідними параметрами еліптичної кривої [12, 9, 32], та мультиплікативну циклічну групу G_2, що також задається стандартно загальними параметрами відповідного розширення поля Галуа $F(p^k)$ [12, 32, 54, 55, 248–253]. Адитивна підгрупа групи G_1 порядку n будується з використанням базової точки P. Метод спарювання будемо позначати ℓ. Уповноважений з генерації використовує головний особистий ключ (майстер-ключ) $S \in Z_q^*$, що приймає цілі значення над указаним полем, для всіх особистих перетворень. Доступним для користувачів є відкритий ключ уповноваженого на генерацію:

$$Q_e = SP. \tag{1.15}$$

Також користувачі повинні узгоджено використовувати два перетворення типу «функція гешування», скажімо H_1 та H_2. Таким чином, множину загальних параметрів, що повинні бути визначеними при здійсненні цифрових підписів, складає вектор параметрів

$$Params = (G_1, G_2, \ell, P, Q_e, H_1, H_2). \tag{1.16}$$

Генерування загальних параметрів G_1 та G_2 зводиться до побудування загальних параметрів відповідної еліптичної кривої, що породжує адитивну групу G_1. До загальних параметрів еліптичної кривої належать: параметри a та b еліптичної кривої, модуль перетворення (просте число або примітивний поліном), порядок кривої U, базова точка P порядку n, а також коефіцієнт зв'язку h, причому $u = hn$. Мультиплікативна підгрупа G_2 зазвичай будується при використанні як загальних параметрів простого числа R або примітивного полінома та первісного елемента поля Θ_v. На цей час спарювання ℓ на еліптичній кривій може бути здійснено з використанням перетворень Вейля і Тейта, а також їх модифікацій. До загальних параметрів відносять також відкритий ключ уповноваженого на генерацію, який обчислюється згідно (1.15). Функції гешування H_1 та H_2 вибираються у відповідності з вимогами застосовного цифрового підпису.

Генерування ключів у системі на ідентифікаторах і спарюванні точок еліптичних кривих здійснюється уповноваженим на генерацію. У його компетенцію може входити генерування загальних параметрів та особистих ключів. Ідентифікатор кожного із користувачів вибирається або призначається згідно з прийнятою політикою безпеки. Уповноважений на генерування обчислює діючий відкритий ідентифікатор, використовуючи ідентифікатор користувача ID згідно з правилом:

$$Q_{ID} = H_1(ID) \in G_1. \tag{1.17}$$

Особистий (асоційований) ключ d_{id} кожного користувача обчислюється уповноваженим на генерацію з використанням особистого ключа S та відкритого ідентифікатора за правилом:

$$d_{id} = SQ_{id} \in G_1. \tag{1.18}$$

Далі відносно відкритого ідентифікатора Q_{id} та особистого ключа d_{id} відповідного користувача має бути забезпечено цілісність, справжність,

доступність і неспростовність, а відносно особистого – ще додатково й високого рівня конфіденційність. Тому особистий ключ повинен бути переданий тільки його власнику по надійно захищеному каналу. Для цього всі користувачі повинні мати з уповноваженим на генерацію захищений канал зв'язку на індивідуальних ключах.

Алгоритм підписування. Кожний підписувач має доступ до загальних параметрів, відкритих та особистого ключа. Підписування здійснюється в такій послідовності.

1. Формується випадкове або псевдовипадкове ціле число $r \in Z_q$, що приймає цілі значення над відповідним полем (r за своєю суттю є особистий ключ сеансу).

2. Обчислюється відкритий ключ сеансу за формулою $U = rP$, який приймає значення точки еліптичної кривої.

3. Обчислюється значення функції гешування від конкатенованих між собою ID, M, U параметрів, тобто:

$$h = H_2(ID, M, U) \in G_1. \tag{1.19}$$

4. Обчислюється підпис повідомлення M:

$$V = d_{id} + rh. \tag{1.20}$$

Підписане повідомлення має такий формат:

$$M, \sigma = \prec U, V \succ \in G_1 * G_1$$

Перевіряння цифрового підпису повідомлення M^*, $\prec U^*, V^* \succ$ здійснюється в такій послідовності.

Обчислюється відкритий ідентифікатор користувача, який підписав повідомлення M:

$$Q_{id} = H_1(ID) \in G_1. \tag{1.21}$$

Обчислюється значення функції гешування від параметрів

$$h^* = H_2(ID, M^*, U^*), \tag{1.22}$$

де символ (*) позначає той факт, що як саме повідомлення M так і підпис V можуть бути викривленими або порушена їхня цілісність.

3. Обчислюються значення $\ell(P, V^*)$, значення $\ell(Q_e, Q_{id})$ та $\ell(U^*, h^*)$. Якщо значення першого спарювання дорівнює добутку двох спарювань, тобто

$$\ell(P, V^*) = \ell(Q_e, Q_{id})\,\ell(U^*, h^*), \tag{1.23}$$

то приймається рішення, що повідомлення M цілісне й справжнє. В іншому випадку воно відхиляється.

1.4. ОСНОВНІ ХАРАКТЕРИСТИКИ ЕЦП

1.4.1. Класифікація ЕЦП

На цей час розроблені й застосовуються ряд алгоритмів (електронного) цифрового підпису, що використовують симетричні або асиметричні методи, різний математичний апарат і дозволяють виробляти та перевіряти підписи одним чи

багатьма суб'єктами в автономному чи інтерактивному режимах, з використанням чи без використання каналів зв'язку [7–10, 15–17, 34, 35]. Деякі з них досліджені й перевірені часом щодо забезпечуваної криптографічної стійкості та швидкості та прийняття як міжнародних [15, 16, 27, 29, 34, 35] чи регіональних стандартів. Наведена нижче класифікація дозволяє визначити властивості будь-якого відомого алгоритму цифрового підпису та зробити порівняння його з іншими алгоритмами, а також визначити по ряду критеріїв кращого з них. Стандартизовані й застосовуються цифрові підписи з додатком [34–37] та цифрові підписи з відновленням повідомлення [27, 29].

Класифікація, на наш погляд, може бути здійснена за такими ознаками та критеріями [7–10].

За кількістю учасників:

а) одиночний – коли в процесі вироблення електронного цифрового підпису достатньо одного учасника;

б) груповий – коли в процесі вироблення цифрового підпису повинно бути більше ніж один учасник. При цьому груповий підпис може здійснюватись:

– із залученням для здійснення цифрового підпису послуги третьої довірчої сторони;

– без залучення третьої довірчої сторони.

За терміном дії ключів:

а) цифрові підписи без терміну обмеження дії ключів;

б) цифрові підписи з терміном обмеження дії ключів.

За способом перевірки:

а) *інтерактивні* – схеми цифрового підпису, що потребують протокольної взаємодії учасників. При цьому інтерактивні цифрові підписи можуть також бути незаперечними. Незаперечні цифрові підписи – це підписи, що не дають можливості перевірки цифрового підпису без дозволу суб'єкта (об'єкта), що підписує;

б) *неінтерактивні* – схеми цифрового підпису, що не потребують протокольної взаємодії учасників.

За способом вироблення підпису:

а) цифровий підпис з відновленням – частина або повне повідомлення може бути відновлене з цифрового підпису;

б) цифровий підпис з додатком – цифровий підпис приєднується до повідомлення і в такому вигляді надсилається адресату;

в) сліпий цифровий підпис – цифровий підпис, що здійснюється без можливості перегляду змісту повідомлення;

г) цифровий підпис за дорученням – який здійснюється довірчим суб'єктом від імені суб'єкта, що довіряє, без надання довірчому суб'єкту таємних ключів суб'єкта, що довіряє;

д) цифровий підпис контракту – коли документ (контракт) підписується одночасно двома підписами (сторонами).

За потребою використання при виробленні цифрового підпису каналу зв'язку:

а) цифрові підписи з інтерактивним каналом зв'язку;

б) цифрові підписи з автономним каналом зв'язку.

За математичною задачею, на якій засновується стійкість цифрового підпису:

а) схеми цифрового підпису, стійкість яких заснована на складності задачі розкладання на співмножники великого числа – модуля перетворення;

б) схеми цифрового підпису, стійкість яких заснована на складності вирішення задачі дискретного логарифму в полях Галуа;

в) схеми цифрового підпису, стійкість яких заснована на задачі дискретного логарифму в групі точок еліптичної кривої;

г) схеми цифрового підпису, стійкість яких заснована на складності вирішення задачі дискретного логарифму в групі точок гіпереліптичної кривої.

За типом криптографічної системи:

а) *симетричні цифрові підписи* – цифрові підписи, що ґрунтуються на симетричних криптографічних перетвореннях з використанням третьої довірчої сторони;

б) *асиметричні цифрові підписи* – цифрові підписи, що ґрунтуються на асиметричних криптографічних перетвореннях і можуть здійснюватись:

– з використанням третьої довірчої сторони;

– без використання третьої довірчої сторони.

За мірою використання криптографічного перетворення типу шифрування:

– цифрові підписи з використанням шифрування;

– цифрові підписи без використання шифрування.

За характером виконуваного цифрового підпису:

– детерміновані цифрові підписи;

– одноразового чи багаторазового застосування;

– цифрові підписи з рандомізацією.

1.4.2. Вимоги до ЕЦП

На основі даних [15–40, 51, 64] ЕЦП мають задовольняти таким вимогам.

1. Алгоритми вироблення та перевірки ЕЦП повинні буди відкритими, тобто нетаємними.

2. Алгоритми вироблення та перевірки ЕЦП повинні мати допустиму для застосувань складність, наприклад, не вище ніж за поліноміальну.

3. Алгоритми знаходження таємного ключа та (або) підробки ЕЦП повинні мати не нижче ніж експонентну (субекспоненційну), тобто практично не реалізовну складність атаки загрози «Повне розкриття».

4. ЕЦП повинен мати чутливість до будь-яких змін підписаних даних, тобто мати максимальну стійкість до виявлення будь-яких змін, підробок і порушень.

5. Вірогідність появи двох однакових підписів для різних повідомлень не повинна перевищувати припустимого значення.

6. Обчислювальні складності вироблення та перевірки ЕЦП повинні бути мінімізовані та мати близькі за величиною значення.

7. ЕЦП мають забезпечувати захист від підробки, підміни та імітації з потрібною ймовірністю як з боку можливого порушника, так і з боку підписувача й одержувача.

8. ЕЦП, що були вироблені для однієї й тієї самої інформації в різний час і на різних засобах (приладах), повинні відрізнятись.

9. Імовірність виникнення колізії, тобто появи для двох різних повідомлень одного й того самого значення ЕЦП, має бути менше заданої допустимої величини, в іншому випадку вони мають відрізнятись одне від одного з великою ймовірністю.

10. Ключі для вироблення ЕЦП повинні бути конфіденційними, а ключі для перевірки ЕЦП мають бути відкритими.

11. Можливість застосування ЕЦП з різними рівнями стійкості та складності вироблення й перевірки ЕЦП.

12. Можливість програмної, програмно-апаратної й апаратної реалізації ЕЦП з приблизно однаковою складністю.

13. Можливість використання ЕЦП як з однаковими загальносистемними параметрами в мережі, так і з індивідуальними для окремих частин об'єктів (суб'єктів) чи доменів.

14. Можливість багаторазового вироблення й перевірки ЕЦП для однієї й тієї самої інформації з використанням різних ключів, різними суб'єктами (об'єктами), а за необхідності з використанням різних загальносистемних параметрів.

15. ЕЦП повинен дозволяти надавати послугу неспростовності (неспростовність відправника, неспростовність джерела, неспростовність транспортування).

16. ЕЦП повинен дозволяти проведення слідчих експериментів з метою забезпечення судового розгляду й арбітражу в разі виникнення суперечок та взаємних непорозумінь.

17. Повинна існувати можливість зберігання ЕЦП як разом із підписаною інформацією, так і окремо від неї.

18. Повинна існувати можливість сліпого підпису, тобто підписування інформації без можливості її перегляду. Наприклад, при видачі електронних карток видається ключ, за допомогою якого користувач має можливість користуватися цією карткою, але при підписуванні цієї інформації людина, яка відповідає за доставку цього ключа, не повинна мати доступ до самого ключа.

19. Повинна існувати можливість «підпису за дорученням», тобто підписування довірчим суб'єктом від імені суб'єкта, що довіряє, без надання довірчому суб'єкту таємних ключів суб'єкта, що довіряє.

20. За необхідністю повинна існувати можливість вироблення «незаперечних підписів», тобто підпису, який може бути перевірений тільки за дозволом суб'єкта (об'єкта), що підписує.

21. ЕЦП повинен бути компактним і займати невеликий обсяг пам'яті.

Наведені вище вимоги до ЕЦП обумовлені необхідністю надання користувачам таких базових послуг, як цілісність, справжність (автентичність), неспростовність і доступність. Більшість з наведених вимог є обов'язковими. У першу чергу необхідно забезпечувати перекриття від існуючих загроз, алгоритми вироблення й перевірки електронних цифрових підписів повинні буди відкритими і мати не вище ніж поліноміальну складність, мати чутливість до будь-яких змін підписаних даних, надавати послугу неспростовності та забезпечувати захист від підробки, підміни та імітації ЕЦП з необхідною ймовірністю як з боку можливого порушника (зловмисника), так і з боку підписувача й одержувача. Алгоритм ЕЦП, що задовольняє переліченим вимогам, здатний забезпечити необхідний рівень стійкості та прийнятні показники часової та просторової складності.

1.4.3. Досвід застосування та основні проблемні питання щодо електронного цифрового підпису

У сучасних автоматизованих системах управління, комп'ютерних системах і мережах, різних інформаційних і телекомунікаційних системах, інформаційно-телекомунікаційних системах, а також системах електронного документообігу висуваються високі вимоги до забезпечення цілісності, автентичності (справжності), неспростовності та доступності інформації (електронних документів) на всіх етапах їх життєвого циклу. При цьому під інформацією будемо розуміти сукупність усіх даних і програм, що використовуються в системі чи технології, незалежно від їхнього логічного чи фізичного подання. Під інформацією розумітимемо також і повідомлення й електронні документи, що циркулюють у відповідних системах чи технологіях. Досвід застосування й проведені дослідження показали, що ці високі вимоги, особливо до реалізації функції неспростовності, можуть бути забезпечені тільки за рахунок застосування ЕЦП. Електронний ЕЦП, по суті, являє собою додані до інформації дані, обчислені за допомогою криптографічного перетворення інформації, що захищається, і параметри, наявність яких дозволяє упевнитися в цілісності й справжності інформації та її джерела, а також забезпечити захист від підробки з боку отримувача.

Власне кажучи, ЕЦП являє собою цифровий еквівалент підпису (штампа, печатки, водяного знаку тощо), наявність якого в повідомленні чи даних програми дозволяє з високою ймовірністю визначити джерело (джерела) цього повідомлення чи даних і юридично довести, що із зазначеною припустимою ймовірністю P_n тільки він міг сформувати цей підпис, але підробити його в процесі заданого часу при обмежених ресурсах зловмисник може з імовірністю, що не перевищує заданої величини P_z. [7–10, 51, 64]. Причому ЕЦП у такий спосіб обчислюється на основі інформації, що захищається, з використанням особистого (конфіденційного) ключа конкретного суб'єкта чи об'єкта, що є його джерелом. Перевірка цілісності й справжності виконується з використанням відкритого ключа, причому знання відкритого ключа не дозволяє підробити ЕЦП з імовірністю, що перевищує P_z.

Наприкінці XX сторіччя протоколи цифрового підпису набули широкого поширення в силу збільшення комп'ютеризації документообігу. Влітку 2000 року президентом США Біллом Клінтоном був підписаний і набув чинності з 1 жовтня наказ «Electronic Signatures in Global and National Commerce Act», що прирівнює в комерційних документах електронний підпис до чорнильного (більш того, і сам цей наказ став першим документом, підписаним електронним цифровим підписом). Європейський Союз прийняв Директиву 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах товариства [5], який вже набув чинності в країнах Союзу. Над ініціативами в цій галузі, взаємодіючи одна з одною, працює багато азіатських держав, причому в деяких із них ЕЦП вже закріплений законодавчо. У Російській Федерації опублікований і доступний по Internet федеральний закон «Про електронний цифровий підпис», а в різних інформаційних системах і технологіях широко застосовується електронний цифровий підпис.

В Україні Закон «Про електронний цифровий підпис» набув чинності з 1 січня 2004 року [2]. Можливість та оперативність його впровадження в Україні

пояснюється також наявністю стандартів ЕЦП [34–37]. Відкритими залишаються питання створення та функціонування інфраструктури відкритих ключів.

Розглянемо історію, етапи створення та досвід застосування ЕЦП на світовому рівні. Історично першим цифровим підписом був підпис, реалізований на основі RSA перетворення [10]. На міжнародному рівні він був закріплений у міжнародному стандарті ISO 11166. У 1991 році через ряд недоліків на зміну RSA прийшов алгоритм DSA, з використанням якого був розроблений стандарт США X 9.30 та FIPS-186 [43], а потім стандарт Російської Федерації ГОСТ Р 34.10-94 та міждержавний стандарт ГОСТ 34.310-95 [40].

Крім доказів теоретичної стійкості ЕЦП, одним з основних факторів є перевірка реально стійкого ЕЦП часом. З часом стало зрозуміло, що вказані ЕЦП, побудовані за алгоритмом Ель-Гамаля [7–10, 51], забезпечують тільки субекспоненційно складність криптоаналізу, а реальне підвищення стійкості є проблематичним. У проекті стандарту IEEE X 9-62 [44] запропонований варіант електронного цифрового підпису, що є модифікацією стандарту X 9.30 (DSA) і отримав назву ECDSA [45]. У ньому як математичний апарат вибрана група точок еліптичної кривої над простим полем. По суті, перехід від DSA до ECDSA дозволив підвищити складність криптоаналізу. У результаті замість асиметричної пари ключів (X_i, Y_i), зв'язаних між собою в полі $F(P)$ співвідношенням

$$Y_i = a^{X_i} (\mathrm{mod}\, P),$$

почали використовувати перетворення в групі точок еліптичної кривої з асиметричною парою ключів (Q_i, d_i), причому

$$Q_i = d_i \cdot G (\mathrm{mod}\, q),$$

де G – базова точка, q – модуль перетворення.

Використання математичного апарату еліптичних груп дозволяє зменшити довжину ключа, що, у свою чергу, дозволяє підвищити швидкість алгоритму формування й перевірки підпису. Найголовніше – це надія на те, що в міру розвитку математичних методів і продуктивності криптоаналітичних систем криптографічні перетворення в групі точок еліптичних кривих будуть більш стійкими до криптоаналізу, ніж перетворення в кільцях і полях. Крім того, при розробці перетворень у групі точок еліптичних кривих з'явилася можливість врахувати вимогу реалізації цифрового підпису з різними довжинами. Природно, що спроби задовольнити суперечливі вимоги до цифрових підписів призвели до потоку розробки різних модифікацій криптоперетворень, у тому числі цифрових підписів.

Абсолютна більшість розроблених у світі ЕЦП базується на використанні асиметричних криптографічних перетворень, що виконуються здебільшого в кільцях, полях Галуа [7–10] і групі точок еліптичних кривих [18–24]. До ЕЦП, реалізованих у кільцях, необхідно віднести RSA-подібні алгоритми, до перетворень у полях Галуа – алгоритми Діффі-Геллмана і Ель-Гамаля. Досвід застосування та проведення досліджень ЕЦП, що базуються на перетвореннях у кільцях і полях, показали, що вони практично вичерпали себе і найближчим часом не забезпечуватимуть необхідної стійкості.

Одним із способів вирішення поставленої задачі є збільшення довжини ключа нині діючих цифрових підписів – RSA і DSA. Однак, збільшення довжини ключа підвищує вимогу цих криптосистем до обчислювальних можливостей ЕОМ, що не

завжди є прийнятним (не всі організації можуть поміняти весь парк комп'ютерів для здійснення прийнятного рівня швидкодії оновлених алгоритмів електронного цифрового підпису). Для вирішення цього протиріччя розроблені й почали впроваджуватися нові модифіковані криптографічні перетворення, що виконуються в групі точок еліптичних кривих. З'явилося значне число методів, на їх основі розроблені стандарти та проекти стандартів [15, 16, 23, 27, 30–36]. Тому важливою й такою, що вимагає вирішення, стала задача вивчення, порівняння, виявлення особливостей та умов застосування, аналізу стійкості та складності здійснення ЕЦП. Основою при порівняльному аналізі, звичайно ж, мають бути вимоги 1–21, що наведені вище. Разом із тим, при виконанні порівняльного аналізу необхідно задатися видами атак і типами загроз ЕЦП відносно інформації, що захищається.

1.4.4. Основні види атак на ЕЦП

Основними видами атак на ЕЦП є такі [7–10, 51, 64, 89–97].

Атака на основі відомого відкритого ключа (key-only attack). Це найслабкіша з атак, вона практично завжди доступна порушнику (криптоаналітику) та може бути реалізованою. Ця атака може виконуватися за умов апріорної визначеності криптоаналітика щодо реалізації ЕЦП, знання загальносистемних параметрів, а також при діючих відкритих ключах.

Атака на основі відомих підписаних повідомлень (known-message attack). Для цієї атаки передбачається, що в розпорядженні криптоаналітика є деяке число пар $(m,\langle r,s\rangle)$ підписаних повідомлень m, при цьому він не може вибирати повідомлення m. Крім того, криптоаналітик знає систему та загальні параметри ЕЦП.

Проста атака з вибором підписаних повідомлень (generic chosen-message attack). У цьому випадку криптоаналітик має можливість вибрати деяку кількість підписаних повідомлень, знає загальносистемні параметри і має після вибору підписаних повідомлень доступ до відкритих ключів.

Спрямована атака з вибором повідомлення (direct chosen-message attack). Криптоаналітик знає загальносистемні параметри, може на власний розсуд вибирати відкритий ключ і після цього вибирати підписані повідомлення.

Адаптивна атака з вибором підписаного повідомлення (adaptive chosen-message attack). При здійсненні атаки криптоаналітик може вибирати відкритий ключ, а також підписане повідомлення. При цьому вибір наступного підписаного повідомлення він може робити на основі знання припустимого підпису попереднього обраного повідомлення.

1.4.5. Основні види загроз ЕЦП

Проведений аналіз показав, що кожна атака спрямована на досягнення певної мети. З урахуванням цього для всіх схем електронних цифрових підписів у порядку зростання небезпеки можна виділити такі види загроз [7–10, 51, 53, 64, 89–94].

Екзистенційна підробка (existential forgery). Загроза полягає у створенні криптоаналітиком для будь-якого, можливо безглуздого, повідомлення m', що відрізняється від перехопленого, реального (правильного) ЕЦП.

Селективна підробка (selective forgery). Являє загрозу створення для заздалегідь обраного повідомлення m правильного ЕЦП.

Універсальна підробка (universal forgery). Ця загроза полягає у виявленні криптоаналітиком алгоритму формування підпису, функціонально еквівалентного дійсному алгоритму ЕЦП, що дозволяє створити чи модифікувати дійсні підписані повідомлення.

Повне розкриття (total break). За цієї загрози криптоаналітик може обчислити особистий ключ підписувача, який, можливо, відрізняється від d, але відповідає відкритому ключу Q. У подальшому це дозволить криптоаналітику формувати цифрові підписи для будь-яких повідомлень і надалі нав'язувати такі хибні повідомлення кореспондентам.

Найбільш надійними є схеми ЕЦП, стійкі проти найслабкіших із загроз на основі найдужчої з атак, тобто проти екзистенційної підробки на основі атаки з адаптивним вибором підписаних повідомлень. Доведено [7, 9, 51, 64], що схеми електронного цифрового підпису, стійкі проти такої атаки, існують тільки тоді, коли існує колізійно стійка однобічна функція (наприклад, геш-функція). Тому можна констатувати, що використання колізійно стійкої геш-функції щонайменше є необхідною умовою захищеності від адаптивної атаки на основі вибраних підписаних повідомлень.

1.5. КІЛЬЦЕВІ ТА ГРУПОВІ ПІДПИСИ

Розглянемо в спрощеному вигляді кільцеві та групові підписи. Їх застосування пов'язане з необхідністю забезпечувати такі послуги, як анонімність при електронному голосуванні, неможливість відстеження витрати грошей в електронних платіжних системах, виконання різних бухгалтерських та адміністративних правомірних дій учасниками певних груп тощо. Також користувачам мають надаватися послуги неспростовності джерела, доставки, телекомунікаційних систем тощо. Одним із механізмів надання послуги неспростовності джерела, представлення і транспортування є електронні цифрові підписи. Будемо розглядати послугу анонімності в сенсі проведення правомірних дій від імені групи з неможливістю визначення ідентифікаційних даних конкретного виконавця. Гарантом підтвердження правомірних дій є послуга неспростовності. Із безлічі розроблених кільцеві та групові підписи дозволяють формувати підписи від імені групи, залишаючи ідентифікаційні дані фактичного підписувача анонімними. Розглянемо деякі визначення понять групового та кільцевого підписів, вимоги до них та їх сутність.

1.5.1. Визначення, вимоги та сутність групових підписів

Фактичним підписувачем називають користувача групи, який формує підпис. У разі кільцевого підпису фактичний підписувач додатково формує групу.

Учасниками підпису називають користувачів групи, що безпосередньо не беруть участі у формуванні підпису.

Результати аналізу групових та кільцевих підписів [135, 167–170] за характеристиками та властивостями подано в табл. 1.2 та 1.3.

Таблиця 1.2. **Порівняльна характеристика групових та кільцевих підписів**

Характеристика	Групові підписи	Кільцеві підписи
Група	– статична; – частково динамічна; – динамічна	Спонтанне створення групи без додаткової ініціалізації
Формування групи	Менеджер групи	Фактичний підписувач
Механізми управління групою	Розподілення таємної інформації (сертифікатів) захищеними каналами зв'язку, база даних для зберігання сертифікатів	Одержання ідентифікаційних даних учасників підпису
Формування підпису	Формується фактичним підписувачем з використанням особистого ключа, одержаного від менеджера групи; сертифікат і повідомлення	Формується фактичним підписувачем, використовуючи особистий ключ, відкриті ключі УП та повідомлення
Гарант дійсності повідомлення	Гарантом формування підпису від імені групи та належності фактичного підписувача до групи є особистий ключ фактичного підписувача та особистий ключ менеджера групи	Гарантом формування підпису від імені групи та належності фактичного підписувача до групи є особистий ключ фактичного підписувача та відкриті ключі користувачів групи
Ідентифікаційні дані фактичного підписувача	Визначення ідентифікаційних даних фактичного підписувача виконується менеджером групи	Неможливо визначити ідентифікаційні дані фактичного підписувача
Незв'язність	незв'язні	– незв'язні; – зв'язні
Математичні методи	– методи нульових знань; – білінійні відображення та проблеми Діффі-Геллмана; – задача дискретного логарифму; – припущення strong RSA; – білінійне відображення	– методи нульових знань; – білінійне відображення та проблеми Діффі-Геллмана; – припущення strong RSA; – білінійне відображення; – криптопримітив; – зведення множини значень в одне; – односпрямована функція з поліноміальною складністю зворотного перетворення при знанні особистого ключа
Границя	– граничні; – один фактичний підписувач	
Розмір підпису	– фіксований; – залежить від розміру групи	

Таблиця 1.3. **Властивості групових і кільцевих підписів**

Властивість	Групові підписи	Кільцеві підписи
Непідробність (unforgeability)	Неможливість формування дійсного підпису користувачем, що не входить до складу групи	
Анонімність (anonymity)	Неможливість визначення ідентифікаційних даних фактичного підписувача. Для групового винятком є менеджер групи	
Границя (threshold)	Найменша кількість підписувачів, що підтверджують документ, використовуючи свої особисті ключі для формування підпису	
Правильність (correctness)	Гарантія підтвердження процедурою *Verify* підпису, що сформований процедурою *Sign*	
Розділимість (separability)	Можливість кожному користувачеві у складі групи обирати криптографічні примітиви та системні параметри за власним бажанням для формування підпису від імені групи	
Зв'язність (linkability)	Незв'язні (unlinkability) – неможливість визначення двох різних підписів, що вироблені однією групою	Можливість визначення двох підписів, сформованих одним фактичним підписувачем навіть при різних групах і повідомленнях
Можливість проглядання (tracebility)	Можливість визначення менеджером групи фактичного підписувача сформованого підпису	Необхідність залучення підмножини D перевірених учасників підпису для унеможливлення визначення ідентифікаційних даних фактичного підписувача
Стійкість до коаліцій (coalition-resistance)	Неможливість формування дійсного групового підпису підгрупою об'єктів, що мають змову (навіть якщо угода між об'єктами однієї групи), де менеджер групи не зміг дізнатися ідентифікаційні дані фактичного підписувача	Неможливість вироблення дійсного підпису коаліцією учасників підпису без знання особистого ключа фактичного підписувача
Стійкість від підробок Non-slanderability	Стійкість від підробок об'єктами інших груп (excupability) – неможливість вироблення справжнього підпису від імені іншої групи користувачами чи менеджером групи, які не входять до складу іншої групи	Неможливість формування справжнього підпису, що буде зв'язаний з підписом, сформованим іншим фактичним підписувачем. Тобто ніхто не зможе сформувати справжній підпис, що зв'язаний із цим підписом (від імені підписувача), за винятком персони, яка дійсно сформувала цей підпис

Новий вид більш «демократичного» групового підпису спростовує роль менеджера групи і надає повноважень щодо управління групою фактичному підписувачу. Визначення ідентифікаційних даних фактичного підписувача може виконувати будь-який користувач групи.

Розглянуті характеристики та властивості кільцевих і групових підписів дозволяють зробити такі висновки.

Менеджер групи виступає гарантом стійкості до підробок підпису з боку користувачів групи, з іншого боку він має доступ до особистих ключів користувачів групи, а також виступає гарантом формування підпису від імені групи й належності фактичного підпису групі, тому потребує повної довіри.

Перевагою кільцевих підписів є можливість спонтанного створення групи фактичного підпису, при цьому гарантом стійкості до підробок підпису з боку користувачів виступає особистий ключ фактичного підписувача та властивість зв'язності. Гарантом дійсності повідомлення є особистий ключ фактичного підписувача, а формування підпису від імені групи – відкриті ключі користувачів групи.

Характерною особливістю граничних кільцевих і групових підписів є згода щонайменше t користувачів з повідомленням, яка виражається у наданні своїх особистих ключів при формуванні підпису.

Властивість зв'язності кільцевих підписів дозволяє залишатися користувачеві анонімним, доки він не зробить протиправних дій. Менеджер групи в груповому підписі забезпечує контроль протиправних дій, але обмежується право на особисте життя, що не сприймається громадою.

1.5.2. Класифікація кільцевих підписів

Згідно [135, 167] кільцеві підписи можна класифікувати за методами побудови алгоритмів:

1) на основі побудування кільця з функціями *trapdoor*;

2) на основі маскування особистого та сеансового ключів;

3) на основі використання криптографічних примітивів зведення множини значень в одне.

Запропонована класифікація дозволяє спростити аналіз швидкісних характеристик, стійкості до атак кільцевих підписів, розподіливши їх на групи за методами побудови. Спрощення досягається за рахунок порівняння однотипних операцій і перевірки стійкості до атак, які притаманні цьому методу.

Загальносистемні параметри для більшості алгоритмів [135, 167–170] представлені таким чином. Уповноважений на генерування ключів (PKG) випадково обирає майстер-ключ $s_m \in Z_q^*$ та обчислює відповідний відкритий ключ $P_{pub} = s_m P$, де $<P>$ генератор циклічної групи G_1 простого порядку q, $<\gamma>$ генератор мультиплікативної групи G_2 простого порядку q. Обирається криптографічна геш-функція $H_1 : \{0,1\}^* \to G_1$ для представлення будь-яких ідентифікаційних даних у відкритий ключ користувача. Додатково обирається криптографічна геш-функція $H_2 : \{0,1\}^* \to Z_q^*$ та білінійне відображення $e : G_1 \times G_1 \to G_2$, що відповідає основним властивостям:

– білінійність:

$\forall P,Q,R \in G_1$, $e(P+Q,R) = e(P,R)e(Q,R)$ та $e(P,Q+R) = e(P,Q)e(P,R)$;

– невирожденість: $e(P,P) \neq 1$;

– ефективність обчислення: існує поліноміальний алгоритм обчислення

$$e(P,Q),\ \forall P,Q \in G_1.$$

Таким чином, загальносистемні параметри подані у вигляді

$$params = \{G_1, G_2, e(.,.), q, P, P_{pub}, H_1, H_2\}.$$

Формування особистого ключа користувача з ідентифікаційними даними $D \in \{0,1\}^*$ виконується *PKG* шляхом $S_{ID} = s_m Q_{ID}$, де $Q_{ID} = H_1(ID)$ – відкритий ключ користувача. Особистий ключ надсилається користувачеві захищеним каналом зв'язку.

Користувачі групи визначаються множиною ідентифікаційних даних $L = \{D_1, D_2 ..., D_n\}$ або множиною відкритих ключів $L' = \{Q_1, Q_2 ..., Q_n\}$.

Наведена класифікація методів побудови кільцевих підписів дозволяє класифікувати всі існуючі підписи для спрощення проведення порівняльного аналізу. Для кожного методу визначена основна ідея побудови підписів і механізми забезпечення послуг неспростовності, дійсності, автентифікації.

Більш детально групові та кільцеві підписи можна знайти в [135, 167] і джерелах, що цитуються в цих роботах.

1.6. ПРОБЛЕМНІ ПИТАННЯ ТА НАПРЯМИ РОЗВИТКУ ЕЦП

Незважаючи на достатньо короткий період існування та застосування ЕЦП, на наш погляд, пройшов складний шлях випробовування як у сенсі визнання й практичного застосування, так і теоретичного розвитку, удосконалення, а також корінного модифікування та зміни поглядів до вимог і теоретичних і практичних оцінок. По суті з 1977 року, уже на практиці змінилося 5 поколінь ЕЦП, перш за все у сенсі зміни використовуваного математичного апарату, а також оперативної стандартизації та впровадження. Дійсно, сьогодні вже існують і впроваджені різною мірою ЕЦП, що реалізовані з використанням математичного апарату теорії кілець (RSA криптографічне перетворення) [10, 7–9, 46, 51], теорії простих і розширених полів Галуа (Ель-Гамаля криптографічне перетворення) [10, 51, 7–9, 40, 43, 46], теорії еліптичних груп над простими та розширеними полями Галуа (Ель-Гамаля криптографічне перетворення) [15, 23, 30–32, 7–10, 44, 52], гіпереліптичних кривих, що ґрунтуються на модифікованих Ель-Гамаля перетвореннях [11], а також ЕЦП, що ґрунтуються на спарюванні (білінійному відображенні) точок еліптичних кривих [12, 132–135, 167–169].

Кожен із названих ЕЦП пройшов свій шлях – від створення до застосування та випробовування часом. На цьому шляху практично основним критерієм застосування та випробовування є його стійкість проти всіх відомих загроз та криптоаналітичних атак.

Так, незважаючи на значне число тверджень і публікацій про зломи RSA криптографічного перетворення [165, 7, 46], алгоритми ЕЦП, що на ньому базуються, продовжують застосовуватися, щоправда з деякими вдосконаленнями та

збільшенням розмірів модулів, наприклад, уже рекомендуються довжини модулів не менше 2048 бітів. Підтвердженням цьому є широке застосування RSA криптографічного перетворення в технологічно розвинених державах і включення його як такого, що може застосовуватися до нових стандартів, наприклад, у FIPS 186-3.

Продовжують застосовувати методи ЕЦП, що базуються на використанні підпису класу Ель-Гамаля, який реалізується з використанням криптографічних перетворень у полях Галуа [46, 4, 7–10]. Причому, якщо раніше застосовували тільки перетворення над простими полями, то сьогодні вже отримали розвиток і застосування над розширеннями полів. Прикладом цьому є широке застосування стандарту [28–29] (DSA), а також стандарту Російської федерації ГОСТ Р 34.10-94 та його міждержавної версії ГОСТ 34.310-95. Також необхідно відзначити, що у версію стандарту FIPS 186-3 включено ЕЦП, що ґрунтується на DSA [46].

Необхідно зазначити, що основним напрямом вдосконалення ЕЦП є використання криптографічних перетворень у групі точок еліптичних кривих за умови застосування алгоритму ЕЦП типу Ель-Гамаля. Цей напрям набув найбільшого розвитку, по суті, в більшості критичних технологій рекомендується застосовувати криптографічне перетворення в групі точок еліптичних кривих над простими та розширеннями полів Галуа. Підтвердженням цьому є прийняття в технологічно розвинених державах ряду стандартів, також їх підтримка на міжнародному рівні. До них необхідно віднести міжнародні стандарти ISO/IEC 15946-2,4, ISO/IEC9796-3, а також ISO/IEC 1488-3. Як національні потрібно назвати федеральний стандарт США FIPS 186-2, 3, стандарт Російської Федерації ГОСТ 34.10-2001, національний стандарт України ДСТУ 4145-2002 тощо. Попередньо можна стверджувати, що ЕЦП, які ґрунтуються на криптографічних перетвореннях у групі точок еліптичних кривих, пройшли випробовування часом і продовжують забезпечувати задекларований рівень стійкості. Це й визначило широке впровадження та застосування криптографічних перетворень у групі точок еліптичних кривих.

Як нові криптоперетворення при реалізації запропоновано криптографічні перетворення в групі гіпереліптичних кривих [11, 165]. У більшості пропозицій є достатні обґрунтування та реалізації. Але їх впровадження, на наш погляд, затримується тим, що особливих переваг над еліптичними кривими вони не мають, а зміна стандартів в інформаційних технологіях – це болючий процес.

Особливий інтерес являє новий клас криптографічних перетворень – спарювання точок еліптичних кривих. Появу цього криптографічного перетворення, перш за все, необхідно пояснити його принциповою відмінністю. У ньому як ключ використовується не сертифікат відкритого ключа, а відкритий ідентифікатор, наприклад, адреса електронної пошти, відкритий ідентифікатор тощо. Інтерес до цього криптографічного перетворення дуже великий, про що свідчить великий потік наукових публікацій і практичних досліджень [158–164, 167–169].

Таким чином, можна стверджувати, що на цей час достатньою мірою розроблена теорія і знайшли застосування ЕЦП, у яких використовуються різний математичний апарат і як наслідок досягаються різні кількісні показники якості, але існують обмеження з точки зору вибору параметрів і генерування асиметричних пар ключів. Дозволяється застосовувати стандарти, що базуються на використанні різного математичного апарату, кожен з яких має свої особливості й обмеження. Є ряд тверджень про слабкість криптографічних перетворень у кільцях і полях.

Окрім того, сьогодні потрібна активна пропаганда ЕЦП, доведення перспективності його застосування та визначення обмежень. Є ряд інших проблемних питань, перш за все практичної реалізації та застосування ЕЦП в інфраструктурах відкритих ключів, генерування асиметричних ключових пар ЕЦП та забезпечення вимог до них тощо.

По суті, розгляд вищезазначених проблемних задач та шляхи їх вирішення наведено в подальших розділах цієї монографії. Так, у 1–5 розділах подано класифікацію, розглядаються вимоги та сутність криптографічних перетворень типу ЕЦП, наводяться методики та результати порівняльного аналізу існуючих систем ЕЦП, надаються відповідні рекомендації та пропозиції щодо їх застосування. У 5 розділі наведені результати класифікації, аналізу та порівняння існуючих функцій гешування, а також розглядаються перспективні функції гешування. Далі в 6–8 розділах наводяться результати класифікації, обґрунтування вимог і порівняльного аналізу криптографічних механізмів і протоколів на основі ЕЦП, розглядаються питання створення та характеристики інфраструктур відкритих ключів технологічно розвинених держав і національної системи ЕЦП, а також проблемні питання цього напряму. Розділи 9–12 присвячено обґрунтуванню (на основі існуючого міжнародного досвіду) вимог до засобів криптографічних перетворень для інфраструктур відкритого ключа, розробці принципів проектування та технологій виготовлення й застосування таких засобів. Розділ 13 присвячений розгляду проблемних питанням ровитку ІВК та систем ЕЦП, а також можливі шляхи їх вирішення.