Розділ 13

ПРОБЛЕМНІ ПИТАННЯ ТА НАПРЯМИ РОЗВИТКУ ІНФРАСТРУКТУР З ВІДКРИТИМИ КЛЮЧАМИ

У цьому розділі наведено актуальні, на наш погляд, теоретичні та практичні проблемні питання. З урахуванням нашого практичного й теоретичного досвіду ми робимо спробу окреслити та прогнозувати напрями розвитку й удосконалення в цілому інфраструктури відкритих ключів.

13.1. ОСНОВНІ ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМНІ ПИТАННЯ

Аналіз розвитку ІВК (PKI) у технологічно розвинених державах та ЄС дозволяє зробити висновок, що проблемні питання та напрями (групи) їх розвитку можна виділити у п'ять основних груп:

1 група – Законодавчого та нормативно-правового регулювання;
2 група – Загально системного рівня;
3 група – Процедурно-функціонального рівня;
4 група – Функціонально-технічного рівня;
5 група – Програмно-технічного рівня.

Серед невирішених теоретичних проблемних питань необхідно виділити такі.

1. Теоретичне обґрунтування та доведення рівнів гарантій ІВК для відображення політик на різних рівнях і в різних ІВК.
2. Теоретичне обґрунтування та розробка концептуальних підходів до вирішення проблем забезпечення інтероперабельності, уніфікації та стандартизації на рівні методів, механізмів, протоколів і технічних специфікацій.
3. Доведення стійкості криптографічних примітивів проти відомих загроз та криптоаналітичних атак, а також безпечності криптографічних протоколів.
4. Удосконалення математичних методів і алгоритмів за критерієм мінімізації складності обчислень, у тому числі засобом паралельного програмування.

5. Визначення напрямів розвитку ІВК, у першу чергу за рахунок теоретичного обґрунтування математичних методів криптографічних перетворень, наприклад, гіпереліптичних кривих, криптоперетворень на ідентифікаторах тощо.

6. Формальне доведення безпечності криптографічних протоколів, у тому числі на ідентифікаторах.

7. Створення науково-методичного апарату й методик порівняння існуючих методів і засобів генерування випадкових і детермінованих випадкових послідовностей і на їх основі ключових даних і системних параметрів.

8. Подальше теоретичне обґрунтування вимог і розробка основоположних принципів і технологій проектування й виготовлення засобів криптографічних перетворень з гарантованим захистом особистих і таємних ключів від компрометації для моделі порушника третього рівня.

Серед проблемних питань практичного спрямування необхідно відзначити такі.

1. Реальне вдосконалення та прийняття всіх складових нормативно-правової бази в галузі інформаційної безпеки – законів, національних, міжнародних і галузевих стандартів, постанов КМУ, наказів і нормативних документів Держспецзв'язку, технічних специфікацій тощо (основний перелік вказаних документів наведено в табл. 13.1).

2. Гармонізація необхідних міжнародних і регіональних стандартів, рекомендацій і технічних специфікацій в Україні, поступове впровадження їх в національну систему ЕЦП.

3. Узгодження ЦСК різних внутрішніх розробників у частині криптографічних механізмів, протоколів управління та сертифікації ключів, технічних специфікацій.

4. Технічне й робоче проектування ЦСК для взаємодії на міжнародному та міждержавному рівнях, дослідна експлуатація й відображення Політик сертифікації на міжнародному та міждержавних рівнях.

5. Забезпечення користувачів на всіх рівнях надійними засобами криптографічних перетворень, у тому числі вищого та середньо-апаратного рівнях.

6. Удосконалення національної системи ЕЦП і трансформування її в національну інфраструктуру відкритих ключів, інтероперабельну також і на міжнародному рівні.

7. Досягнення беззбиткового функціонування системи ЕЦП в комерційному секторі.

8. Створення системи підготовки та перепідготовки кадрів для системи ЕЦП.

9. Забезпечення необхідної координації дій органів державної влади, перш за все контролюючого органу, центрального засвідчувального органу та розробників.

10. Більш ефективне використання держбюджетного фінансування та матеріально-технічних ресурсів, залучення інвестицій до розвитку ІВК в цілому, включаючи систему ЕЦП.

У таблиці 13.1 наведено дані щодо стану нормативно-правового забезпечення системи ЕЦП України.

Таблиця 13.1. **Нормативно-правове забезпечення ЕЦП України**

Закони України	«Про інформацію» № 2657 від 02.10.1992
	«Про захист інформації в АС» від 05.07.1999
	«Про ЕЦП» № 852 від 22.05.2003
	«Про електронні документи та ЕДО» № 852 від 22.05.2003
	«Про ДССЗЗІ України» № 3475 від 23.02.06
Накази Президента України	«Про Положення про порядок здійснення криптографічного захисту інформації в Україні» № 505 від 22.05.1998
	«Питання ДСТСЗІ СБ України» № 1120/2000 від 06.10.2000
Постанови Кабінету Міністрів України	«Про затвердження Порядку засвідчення наявності електронного документа на певний момент часу» № 680 від 26.05.2004
	«Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади» № 1453 від 28.10.2004
	«Про затвердження Положення про центральний засвідчувальний орган» № 1451 від 28.10.2004
	«Про затвердження Порядку обов'язкової передачі документованої інформації» № 1454 від 28.10.2004
	«Про затвердження Порядку застосування ЕЦП органами державної влади...» № 1452 від 28.10.2004
	Постанови КМ України в галузі ТЗІ
Накази СБУ та ДССЗЗІ України	«Про затвердження Тимчасової інструкції про порядок постачання і використання ключів до засобів КЗІ» № 708/156 від 28.11.1997
	«Про затвердження Положення про державну експертизу у сфері КЗІ» № 62 від 25.12.2000
	«Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням ЕЦП» № 141 від 20.07.2007
	«Про затвердження Інструкції про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави» № 45 від 22.10.1999
	«Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису» № 143 від 24.07.2007
	«Про затвердження Правил посиленої сертифікації» № 3 від 13.01.2005 (в редакції Наказу ДСТСЗІ СБУ № 50 від 10.05.2006)
	«Про затвердження Інструкції про порядок постачання і використання ключів до засобів КЗІ» № 114 від 12.06.2007
	«Про затвердження Ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів КЗІ, надання послуг у галузі КЗІ...» № 8/216 від 26.01.2008

13.2. ІСНУЮЧІ ТА ПЕРСПЕКТИВНІ МЕТОДИ КРИПТОПЕРЕТВОРЕНЬ ДЛЯ ЕЦП

У розділах 1–4 розглянуто основні методи криптографічних перетворень, що застосовуються в системах ЦП. Нині також розглядаються ряд перспективних напрямів, що пов'язані перш за все із застосуванням криптографічних перетворень на ідентифікаторах зі спарюванням точок еліптичних кривих і на гіпереліптичних кривих. Можливість та умови застосування вказаних перетворень вивчені теоретично, створені та випробовуються дослідні версії, розроблено рекомендації та обговорюється необхідність створення регіональних і міжнародних стандартів. У зв'язку з вищезазначеним вважаємо за необхідне розглянути ці криптографічні перетворення дещо детальніше.

Розгляд розпочнемо з таблиці 13.2, у якій наведено основні асиметричні криптоперетворення, що застосовуються або можуть застосовуватись для таких криптографічних перетворень, як (електронний) цифровий підпис, направлене шифрування й узгодження ключів. До них належать криптографічні перетворення:

– у кільцях (наприклад, RSA перетворення) – (перший рядок);
– у полях Галуа (другий рядок);
– у групі точок еліптичних кривих (третій рядок);
– на гіпереліптичних кривих (четвертий рядок);
– зі спарюванням точок еліптичних кривих (п'ятий рядок).

У другому стовпчику таблиці 13.2 наведено ідентифікатори особистих ключів, у третьому – відкритих ключів, у четвертому – вже повністю асиметричні пари відповідних криптографічних перетворень, у п'ятому – загальні параметри асиметричних перетворень, а в шостому – оцінки стійкості проти атак «Повне розкриття». В останньому рядку наведено ідентифікатори сертифікатів відкритих ключів для відповідних криптографічних перетворень.

Як випливає з таблиці 13.2, в якості сертифіката відкритого ключа електронного цифрового підпису в RSA системі використовується D_i ключ із асиметричної пари ключа (D_i, E_i), а як особистий ключ електронного цифрового підпису – ключ E_i.

Для асиметричного криптографічного перетворення в полі Галуа як сертифікат відкритого ключа електронного цифрового підпису використовується елемент поля Y_i, а як особитий ключ – ціле число X_i.

Для асиметричного криптографічного перетворення в групі точок еліптичних кривих як сертифікат відкритого ключа електронного цифрового підпису використовується точка еліптичної кривої Q_i, а як особистий ключ електронного цифрового підпису – ціле число d_i.

При застосуванні криптографічного перетворення на гіпереліптичних кривих як сертифікат відкритого ключа використовується якобіан D_2, а як особистий ключ – якобіан D_1.

При застосуванні криптографічного перетворення зі спарюванням точок еліптичних кривих як сертифікат відкритого ключа електронного цифрового підпису використовується Q_{iD}, а як особистий ключ – d_{iD}.

Таблиця 13.2. **Асиметричні криптографічні перетворення для ЕЦП**

Параметри перетворення / Вид перетворення	Особистий ключ	Відкритий ключ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри	Сертифікати	Складність криптоаналізу
Перетворення в кільці (RSA)	E_i	D_i	(E_i, D_i)	$N = PQ$	D_i	Субекспоненційна
Перетворення в полі Галуа $F(P)$ (DSA)	X_i	$Y_i = g^{X_i} (\text{mod } P)$	(X_i, Y_i)	P, q, g	Y_i	Субекспоненційна
Перетворення в групі точок еліптичних кривих $E(F(q))$	d_i	$Q_i = d_i G (\text{mod} q)$	(d_i, Q_i)	$a, b, G, n,$ $f(x)(P), h$	Q_i	Експоненційна
Перетворення в гіпереліптичних кривих	C_i	$D_2 = c_i D_1$	(c_i, D_2)	$f(x), g(x), q,$ D_1, g, J	D_2	Експоненційна
Перетворення зі спарюванням точок еліптичних кривих	$d_{ID} =$ $= s\, Q_{ID}$	$Q_{ID} = H_1(ID)$	$(d_{ID},$ $Q_{ID})$	$G_1, G_2, e,$ $H_1, P, H_2,$ $H_3,$ F_2^m, P_p	Q_{ID}	Міжекспоненційна – субекспоненційна

Сутність і якість застосування криптографічних перетворень у кільцях, полях Галуа та в групах точок еліптичних кривих наведено в розділах 1–5 цієї монографії. Що стосується криптографічних перетворень у гіпереліптичних кривих та зі спарюванням точок еліптичних кривих, то основні положення та властивості таких підписів розглянемо нижче.

13.3. КРИПТОПЕРЕТВОРЕННЯ В ГІПЕРЕЛІПТИЧНИХ КРИВИХ

Першими пропозиціями щодо застосування гіпереліптичних кривих вочевидь необхідно вважати пропозиції Neal Koblitz – професора математики Вашингтонського університету [11]. Він є визнаним математиком, у тому числі з алгебраїчної геометрії, що включає й розділи теорії еліптичних і гіпереліптичних кривих. Деякий час вважалося, що застосування перетворень на гіпереліптичних кривих ц криптографії суттєво обмежено через складності необхідних обчислень і, як наслідок, незадовільний рівень швидкодії.

Значні результати у вирішенні цього протиріччя вніс професор Christof Paar (Германія). Ним вирішені задачі оптимізації обчислень на гіпереліптичних кри-

вих 1–4 родів [237–240]. Так, він виконав оптимізацію формул складання та подвоєння дивізорів з використанням узагальненого метода Карацуби. Це дозволило підвищити швидкодії перетворень на гіпереліптичних кривих, досягти результатів, порівнюваних зі складністю перетворень на еліптичних кривих, а в деяких випадках і перевершити їх. Він також вів модифіковану метрику, більш точну. Останні дослідження значною мірою присвячені оптимізації складання та подвоєння за критерієм складності [237–244]. В останні роки значні зусилля були спрямовані й на розробку теорії та практики криптографічної стійкості відносно криптографічних перетворень на гіпереліптичних кривих [237–240, 243].

Визначено, що основним параметром, від значення якого залежить криптографічна стійкість перетворень на еліптичних кривих, є порядок групи дивізорів гіпереліптичної кривої. На сьогодні для визначення порядку еліптичної кривої можуть бути застосовані два класи методів – *l*-адичні та *p*-адичні. В обох випадках теоретичною основою є поняття Дзета-функції та гіпотези Вейля. Чисельником Дзета-функції є характеристичний поліном ендоморфізма Фробеніуса. Далі, якщо гіпереліптична крива визначена над кінцевим полем $GF(q)$, то для визначення її порядку достатньо знати число точок, які задовольняють рівнянню кривої над усіма розширеннями поля $GF(q)$ до $GF(q^g)$ включно, де g – рід кривої. Нині найбільше розповсюдження отримали *p*-адичні методи визначення порядку гіпереліптичних кривих.

Наведемо деякі поняття й визначення, що стосуються гіпереліптичних кривих, орієнтуючись на [237–244].

Визначення 13.1. Нехай F – кінцеве поле та нехай $\overline{F}$ – алгебраїчне замикання F. Тоді рівняння вигляду:

$$C:\ y^2 + h(x)y = f(x)\ F[x, y], \tag{13.1}$$

де $h(x) \in F[x]$ – поліном степені не більше g, $f(x) \in F[x]$ – нормований поліном степені $2g + 1$ і не має розв'язків $(x, y) \in F \times F$, які одночасно задовольняли б рівнянню $y^2 + h(x)y = f(x)$, і рівняння приватних похідних задовольняють умовам $2y + h(x) = 0$ та $h'(x)y - f'(x) = 0$, визначає гіпереліптичну криву C роду $g (g \geq 1)$ над F.

Коли $g = 1$, то ми маємо звичайну еліптичну криву. У цьому випадку нормований поліном $f(x) \in F[x]$ у рівнянні (13.1) є поліномом третього ступеню.

За цієї умови еліптична крива E в канонічній формі Веєрштрасса в афінних координатах може бути подана в такому вигляді:

$$E:\ y^2 = x^3 + ax^2 + bx + c, \tag{13.2}$$

причому коефіцієнти $a, b, c \in F$. Також відомо, що гіпереліптична крива не має особливих точок.

Нехай $P = (x, y)$ – кінцева точка на гіпереліптичній кривій C. Протилежною точці P є точка $\tilde{P} = (x, -y - h(x))$. Також точка на нескінченності P_∞ є протилежною сама собі, тобто $P_\infty = -P_\infty$. Якщо кінцева точка задовольняє умові $P = \tilde{P}$, то така точка називається точкою спеціального вигляду, усі інші називаються звичайними.

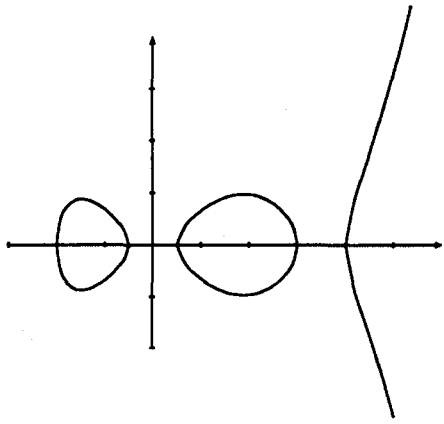

Рис. 13.1. Гіпереліптична крива над полем дійсних чисел R

На рис. 13.1 наведено приклад гіпереліптичної кривої над полем дійсних чисел.

Для такої кривої точка на нескінченності лежить у проективній площині $P^2(F)$. Це єдина точка, що лежить на прямій у нескінченності, що задовольняє рівнянню, однорідному рівнянню гіпереліптичної кривої. Якщо $g \geq 2$, то P_∞ є єдиною особливою точкою.

Як групова структура для гіпереліптичних кривих розглядається якобіан кривої C. Кожен елемент якобіана – це клас еквівалентності дивізорів. Розглянемо поняття дивізорів та їх основні властивості.

Визначення 13.2. *Дивізор* D – це кінцева формальна сума точок гіпереліптичної кривої $P_i \in C$, яка визначається таким чином:

$$D = \sum_{P_i \in C} m_i P_i, \quad m_i \in Z, \tag{13.3}$$

якщо тільки кінцеве число m_i не дорівнює нулю.

Степінь D позначається як $\deg D$. Воно є цілим числом, яке визначається як $\sum_{P_i \in C} m_P$. Порядком $ord_P(D) = m_P$ дивізора D в точці P є ціле число m_P – таке, що порядок дивізора в точці P є m_P.

Визначення 13.3. Кількість точок дивізора називається *вагою дивізора*.

Множина всіх дивізорів D формує адитивну групу з операцією складання:

$$\sum_{P_i \in C} m_i P_i + \sum_{P_i \in C} n_i P_i = \sum_{P_i \in C} (m_i + n_i) P_i. \tag{13.4}$$

Множина D^0 позначає підгрупу D, яка складається з дивізорів нульового степеня.

Визначення 13.4. Нехай $R = \in \overline{F}(C)^*$. Дивізором раціональної функції R є

$$div(R) = \sum_{P \in C} (\mathrm{ord}_p R) P. \tag{13.5}$$

Тобто дивізор раціональної функції – це кінцева формальна сума, що має степінь 0.

При визначенні якобіану гіпереліптичної кривої використовується поняття *головний дивізор.*

Визначення 13.5. Дивізор $D \in D^0$ називається *головним дивізором,* якщо $D = div(R)$ для певної раціональної функції $R = \in \overline{F}(C)^*$. Множину всіх головних дивізорів позначають як P.

Нехай f є функція. Дивізор $div(f)$ можна подати у вигляді різниці двох дивізорів:

$$div(f) = div_0(f) - div_\infty(f), \tag{13.6}$$

де $div_0(f)$ відповідає перетинанню C з кривою $f = 0$ і $div_\infty(f)$ – перетинанню C з кривою $\frac{1}{f} = 0$.

Наведемо також визначення якобіана гіпереліптичної кривої.

Визначена згідно з 13.6 фактор-група

$$J = D^0 / P \tag{13.7}$$

називається *якобіаном гіпереліптичної кривої* C.

Якщо D_1, $D_2 \in D^0$ і $D_1 - D_2 \in P$, то зазвичай позначають $D_1 \sim D_2$. У цьому випадку D_1 і D_2 називають *еквівалентними дивізорами*. Тобто якобіан являє собою кінцеву фактор-групу однієї нескінченної групи за іншою нескінченною групою. Кожен елемент якобіана є класом еквівалентності дивізорів.

Розглянемо сутність геометричного закону складання дивізорів гіпереліптичної кривої [242].

Якобіан гіпереліптичної кривої другого роду включає дивізори, що утворені однією або двома точками. Виходячи з визначення якобіана, для того щоб побудувати групу, необхідно утворити фактор-групу сум точок на кривій за підмножиною сум тих точок, що лежать на функції.

В абелевій групі, якою є якобіан гіпереліптичної кривої, головною операцією, що визначає складність, є процесс обчислення кратного cD для великих цілих чисел c:

$$cD = \underbrace{D + D + \ldots + D}_{c \text{ разів}}. \tag{13.8}$$

Ця операція називається скалярним множенням дивізора на число і вимагає для її реалізації додавання та дублювання дивізорів.

Стійкість криптографічних систем ґрунтується на великій (експоненційній) складності вирішення зворотної задачі – дискретного логарифмування в якобіані гіпереліптичної кривої [11, 245].

Для виконання групових операцій в якобіані гіпереліптичної кривої застосовується базова ітераційна формула Кантора [245]. Вона є дійсною для гіпереліптичних кривих довільного роду і може бути заданою у вигляді такого двохкрокового алгоритму.

Знаходиться напівприведений дивізор $D' = div(u', v')$ – такий, що $D' \sim D_1 + D_2 = div(u_1, v_1) + div(u_2, v_2)$ у групі J [ ].

Напівприведений дивізор $D' = div(u', v')$ зводиться до еквівалентного приведеного дивізора $D = (u, v)$.

Детальні дані щодо складності виконання групових операцій в якобіані гіпереліптичної кривої можна знайти в [237, 240, 242].

13.4. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ГІПЕРЕЛІПТИЧНИХ КРИВИХ ДЛЯ ЕЦП

Основним проблемним питанням при застосуванні гіпереліптичних кривих є доведення криптографічної стійкості проти атаки «Повне розкриття». Вона формулюється таким чином. Задано дивізор D_1, що генерує циклічну підгрупу

якобіана гіпереліптичної кривої. Також $D_2 \in <D_1>$. Необхідно знайти ціле число C, для якого виконується умова:

$$D_2 = cD_1. \tag{13.9}$$

Як показано у [246, 112], порядок якобіану гіпереліптичної кривої обмежений інтервалом Хассе-Вейля:

$$\left|(\sqrt{q}-1)^q\right| \le \#J/GF(q) \le \left\lfloor(\sqrt{q}+1)^{2g}\right\rfloor, \tag{13.10}$$

де q – характеристика поля, над яким визначено криву, а g – рід кривої. Тому можна вважати, що порядок якобіану має таку наближену оцінку:

$$\#J/GF(q) \approx q^8. \tag{13.11}$$

Також показано [246], що для гіпереліптичної кривої роду 2 з довжиною операндів 80 бітів, для кривих роду 3–40 бітів.

У [238, 243] стверджується, що показники стійкості для еліптичних і гіпереліптичних кривих будуть однаковими для однакових порядків. При цьому довжина елемента основного поля зменшується пропорційно роду кривої. Але потрібно враховувати, що складність формул групової операції зростає зі збільшенням роду кривої.

Орієнтуючись на роботу, покажемо як реалізувати ЕЦП ДСТУ 4145-2002 на основі групи дивизорів (якобіану) гіпереліптичної кривої [247]. Це можна зробити модифікуючи протокол ЕЦП із [35], підставивши замість точок еліптичної кривої дивізори гіпереліптичної кривої (табл. 13.3).

Таблиця 13.3. **Алгоритми ЕЦП згідно з ДСТУ 4145-2002 на гіпереліптичній кривій**

Алгоритм вироблення підпису	Алгоритм перевірки підпису
Вхід: Особистий ключ d, відкритий ключ – дивізор $Q = -d \times D$, загальносистемні параметри. Вихід: Значення ЕЦП $\langle r, s\rangle$ для певного повідомлення M	Вхід: Відкритий ключ – дивізор Q, загальносистемні параметри, цифровий підпис $\langle r', s'\rangle$ для певного повідомлення M'. Вихід: Підпис дійсний або ні
1. Обчислити геш-значення $h = H(M) \bmod n$. 2. Генерація випадкового $k \in \{1,\ldots,n-1\}$. 3. Обчислити $R = k \times D$. 4. Обчислити $F_e = \psi(R) \bmod n$. 5. Обчислити відкритий ключ сеансу $r = F_e \bmod n$. 6. Обчислити значення підпису $s = (k + dr) \bmod n$.	1. Обчислити геш-значення $h' = H(M') \bmod n$. 2. Обчислити $R' = s' \times D + r' \times Q$. 3. Обчислити $y = \psi(R') \bmod n$. 4. Обчислити $v = h'y$. 5. Перевірити, чи $r' = v$.

При обчисленнях як загальносистемні параметри використовуються базовий дивізор D і порядок базового дивізора n. Як і раніше, $H(M)$ – геш-функція, а $\psi(R)$ – функція перетворення дивізора на елемент основного поля.

Аналізуючи дані таблиці 13.3, можна зробити висновок, що модифікація криптоперетворення типу ЕЦП ДСТУ 4145-2002 може бути зведена до заміни точок еліптичної кривої на групу дивізорів, тобто якобіан, гіпереліптичної кривої. При цьому в разі використання гіпереліптичних кривих і застосування несуперсингулярних гіпереліптичних кривих 2 та 3 родів досягають показники криптографічної стійкості аналогічного порядку, як і на еліптичних кривих.

У цілому можна прогнозувати, що якщо з часом будуть знайдені ефективні атаки на криптографічні перетворення в групі точок еліптичних кривих, наприклад «Повне розкриття», то на зміну можуть прийти гіпереліптичні криві.

13.4.1. Введення в асиметричну криптографію на ідентифікаторах

Як відомо, в асиметричних криптографічних системах пари ключів складаються з особистого та відкритого ключів. Наприклад, у системах, що базуються на перетвореннях у групі точок еліптичних кривих, – це пара (d_i, Q_i), де d_i – особистий ключ, а Q_i – відкритий ключ (сертифікат). Сутність застосування таких асиметричних пар ключів наведена вище в розділах 1–5. Нині, на наш погляд, у середовищі спеціалістів ведуться інтенсивні досліджедження та пошукові роботи в напрямку створення ІВК на ідентифікаторах і комбінованих ІВК [248–260].

Одним із основних завдань асиметричної криптографії, що базується на ідентифікаторах, є виключення необхідності виготовлення й обслуговування сертифікатів відкритих ключів принаймні кінцевим користувачем.

Основною перевагою такого підходу є можливість застосування замість відкритого ключа (сертифіката) особистої ідентифікаційної інформації. Такою ідентифікаційною інформацією може виступати адреса електронної пошти, IP-адреса на мережному рівні тощо. Така адреса може бути представлена у вигляді бінарного ідентифікатора ID э {1,0}, Можливі й інші подання ідентифікаційної інформації.

Особистий (закритий, таємний) ключ генерується та розподіляється між користувачами, уповноваженим на генерацію (УГ). Уповноважений на генерацію має свій головний (майстер) ключ, використовуючи який уповноважений генерує особисті ключі користувачів, якщо вони звертаються до нього за цією послугою. Оскільки особистий ключ повинен бути пересланий від уповноваженого на генерацію користувачеві, то всі користувачі повинні мати з уповноваженим на генерацію захищений канал зв'язку на індивідуальних ключах. Якщо порівняти, то майстер-ключ уповноваженого на генерацію за важливістю є таким самим, як і особистий ключ уповноваженого на сертифікацію ІВК (центра сертифікації).

Відзначимо, що для системи на базі ідентифікаторів обов'язковим є виконання таких вимог (рис. 13.2):

Користувач (відправник) A повинен бути повністю впевненим у правильності ідентифікатора того, хто отримує, тобто сторони B;

Уповноважений на генерування повинен встановити (передати) особистий (закритий) ключ тільки стороні отримання B.

Як показав аналіз [250, 54, 55], криптографія на базі ідентифікаторів головним чином заснована на «новому» криптографічному примітиві – спарюваннях (парному відображенні) на еліптичних кривих. Математичні основи спарювання точок на еліптичній кривій були відомі математичному співтовариству ще з 1972 року. Але нове практичне застосування було закладене тільки в роботах Boneh–Franklin, Joux [250]. Спарювання має дуже важливу властивість, яка має назву *білінійність*. Якраз на базі білінійності ґрунтується його нове криптографічне застосування.

У цілому щодо криптографії на базі ідентифікаторів можна зробити такі попередні висновки:

1. Застосування криптографії на ідентифікаторах дозволяє суттєво спростити ІВК за рахунок відмови від використання сертифікатів. У цьому випадку немає необхідності в обслуговуванні, управлінні, створенні, видаленні та розподіленні сертифікатів. Указане в свою чергу призводить до зменшення витрат на управління інфраструктурою відкритих ключів і робить системи управління ключами більш масштабними.

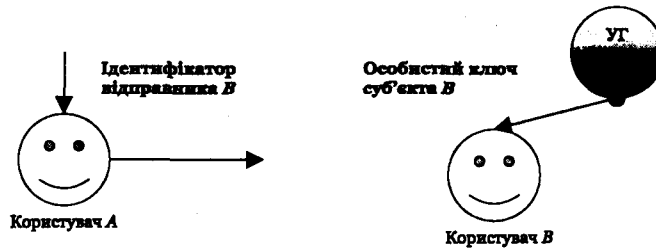

Рис. 13.2. Приклад функціонування криптографічної системи на базі ідентифікаторів

Зменшення числа складних компонентів (директорій) інфраструктури. При цьому користувач-відправник не має необхідності попередньо перевіряти відкритий ключ сторони, яка отримує.

Автоматичне скасування (анулювання) компрометованих ключів. За рахунок застосування відповідної політики безпеки ідентифікатор користувача може мати певний період життя і бути автоматично зміненим. Така властивість може бути забезпечена за рахунок використання розширеного ідентифікатора. Відповідно особистий ключ в кінці кожного періоду теж скасовується (анулюється). Причому для автоматичного анулювання нема необхідності впроваджувати такі сервіси, як CRL, тощо.

13.5. МЕТОД ШИФРУВАННЯ НА БАЗІ ІДЕНТИФІКАТОРІВ

Розглянемо перший метод шифрування на базі ідентифікаторів на прикладі Identity Based Encryption (IBE), який був запропонований у 2001 році авторами роботи [250] (Boneh-Franklin). По суті, вказаний метод є реалізацією протоколу направленого шифрування на ідентифікаторах. Безпека протоколу шифрування базується на складності вирішення білінійної проблеми Діффі-Геллмана (BDHP) [253, 260]. Будемо вважати, що загальні параметри розповсюджуються згідно з безпечними протоколами.

Ідея шифрування базується на основній властивості скалярного відображення – його білінійності. Вона полягає в тому, що для деяких точок еліптичної кривої B і D, а також цілих a та c є справедливим таке:

$$Спарювання(a \bullet B, c \bullet D) = Спарювання(c \bullet B, a \bullet D). \quad (13.12)$$

Розглянемо протокол направленого шифрування на ідентифікаторах з використанням спарювання точок еліптичних кривих. Нехай відправником є користувач A і він здійснює зашифрування для користувача B. Будемо вважати, що користувачі мають доступ до загальних параметрів, що ними використовуються та забезпечується їх цілісність і справжність. Реалізуючи за шифрування, зробимо спробу повторити протокол направленого шифрування, що використовується в ІВК.

На першому етапі користувач A формує випадкове число r та, знаючи загальну для користувачів базову точку P на еліптичній кривій, обчислює відкритий ключ сеансу:

$$R = r \bullet P. \quad (13.13)$$

Випадкове число r по суті є особистим (таємним) ключем сеансу, воно повинне вибиратись із умови $0 < r < n$, де n – порядок базової точки. Як результат, виконуючи обчислення згідно з (13.13), одержуємо значення точки R на еліптичній кривій. Це значення можна вважати еквівалентом відкритого ключа сеансу передачі зашифрованого повідомлення. Рекомендується $1 < r < n - 1$.

Далі користувач A повинен виробити ключ за шифрування, використовуючи властивість спарювання (13.12). Він вибирає як параметри (13.12) такі:

$$a = r, B = ID\,b, c = s, D = P \quad (13.14)$$

та обчислює таємний ключ сеансу

$$k = Спарювання(r \bullet D_B, s \bullet P), \quad (13.15)$$

причому sP він отримує як загальний параметр.

Як конкретний практичний метод спарювання в залежності від конкретної специфіки (тип кривої, величина параметрів тощо) для обчислення k може бути використаним спарювання Вейля або спарювання Тейта.

За умови узгодження між користувачами алгоритму, шифрування та зашифрування повідомлення M користувач A може здійснити, використовуючи таємне значення k. Як правило, значення k у явному вигляді використовувати не можна. Тому необхідно використати відповідним чином узгоджену функцію вироблення ключа (ФВК), наприклад, функцію гешування. Таким чином таємний ключ сеансу (K_c) шифрування виробляється як:

$$K_c = \text{ФВК}\,(k) \quad (13.16)$$

Насамкінець користувач здійснює зашифрування повідомлення M та отримує криптограму:

$$C = E\,(K_c, M), \quad (13.17)$$

яку разом з відкритим ключем сеансу R передає користувачеві B.

Розглянемо розшифрування криптограми користувачем B. Отримавши зашифроване повідомлення, користувач B робить запит уповноваженому на генерацію та отримує від нього по захищеному каналу особистий ключ розшиф-

рування s. Використовуючи цей ключ, користувач B обчислює параметр спарювання k за правилом:

$$k = Спарювання(s \bullet D_B, r \bullet P), \tag{13.18}$$

а потім таємний ключ сеансу K_c. На останок, використовуючи узгоджений алгоритм розшифрування, користувач B здійснює розшифрування криптограми й отримує відкрите повідомлення:

$$M = D(K_c, C). \tag{13.19}$$

Проведемо аналіз алгоритму шифрування щодо його порівняння з відомими алгоритмами направленого шифрування з використанням асиметричної пари із сертифікатом інфраструктури ІВК.

Алгоритм, що розглядається, можна віднести до алгоритму направленого шифрування, оскільки зашифрування здійснюють з використанням загальнодоступного ідентифікатора-еквівалента відкритого ключа. Проблемним тут є питання забезпечення цілісності й справжності ідентифікатора. Якщо відносно особистого ключа забезпечується відповідний режим, то розшифрування також можна вважати направленим. Але в цьому випадку необхідно забезпечити захист від зловмисних дій уповноваженого на генерацію та захищений канал передачі таємного ключа s від уповноваженого до користувача, що виконує розшифрування (у нашому випадку користувач B).

13.6. ЦИФРОВИЙ ПІДПИС НА БАЗІ ІДЕНТИФІКАТОРІВ

При викладенні сутності та можливостей ЕЦП будемо дотримуватись термінології, призначення й основних положень, що є визнаними відносно ЕЦП у звичайній системі ІВК.

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

До загальних параметрів будемо відносити адитивну групу G_1, що задається стандартно відповідними параметрами еліптичної кривої, та мультиплікативну циклічну групу $r = F_e \bmod G_2$, що також задається стандартно загальними параметрами відповідного розширення поля Галуа $F(p^k)$ [257, 258]. 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:

$$Q_в = SP. \tag{13.20}$$

Також користувачі повинні узгоджено використовувати два перетворення типу функція гешування, скажімо H_1 та H_2. Таким чином, множину загальних параметрів, яку треба визначити при здійсненні цифрових підписів, складає вектор параметрів:

$$Params = (G_1, G_2, \ell, P, Q_в, H_1, H_2). \tag{13.21}$$

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 відносять: 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 в якості загальних параметрів простого числа R або примітивного полінома та первісного елемента поля θ_v. На сьогодні спарювання ℓ на еліптичній кривій може бути здійснене з використанням перетворень Вейля та Тейта, а також їх модифікацій. До загальних параметрів відносять також відкритий ключ уповноваженого на генерацію, який обчислюється згідно з (13.20). Функції гешування H_1 та H_2 вибираються у відповідності з вимогами цифрового підпису, що застосовується.

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:

$$Q_{ID} = H_1(ID) \in G_1. \tag{13.22}$$

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

$$d_{id} = SQ_{id} \in G_1. \tag{13.23}$$

Далі відносно відкритого ідентифікатора Q_{id} та особистого ключа d_{id} відповідного користувача мають бути забезпечені цілісність, справжність, доступність і неспростовність, а відносно особистого ще додатково й високого рівня конфіденційність. Тому особистий ключ повинен бути переданий тільки його власникові 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 особистим ключем сеансу).

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

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

$$h = H_2(ID, M, U) \in G_1. \tag{13.24}$$

4. Обчислюється підпис повідомлення M:

$$V = d_{id} + rh. \tag{13.25}$$

Підписане повідомлення має такий формат:

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

Перевіряння цифрового підпису

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

1. Обчислюється відкритий ідентифікатор користувача, який підписав повідомлення M:

$$Q_{id} = H_1(D) \in G_1. \tag{13.26}$$

2. Обчислюється значення функції гешування від параметрів

$$h^* = H_2(D, M^*, U^*), \tag{13.27}$$

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

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

$$\ell(P, V^*) = \ell(Q_b, Q_{id})\, \ell(U^*, h^*), \tag{13.28}$$

то приймається рішення, що повідомлення M цілісне та справжнє. Інакше воно відхиляється.

13.7. МЕТОД ЕЦП ІЗ ВИКОРИСТАННЯМ ІДЕНТИФІКАЦІЙНИХ ДАНИХ НА ОСНОВІ СТАНДАРТУ ДСТУ 4145-2002

При викладенні матеріалу будемо спиратися на результати робіт [15, 248–252], у тому числі й наші [254–258].

Оскільки використовується симетричне спарювання Тейта, вважатимемо, що задані:

– G_1 – адитивна група точок еліптичної кривої простого порядку n над розширеним полем характеристики 2;

– G_2 – підгрупа мультиплікативної групи скінченного поля з порядком, як у групи G_1;

– e – парне відображення Тейта;

– геш-функція H_1:{0,1} → G_1, що відображує ідентифікатор користувача в точку на еліптичній кривій;

– геш-функція H_2:{0,1}* → F_2^m, що відображує повідомлення користувача в елемент скінченого поля;

– геш-функція H_3: $G_2 \to F_2^m$.

Також при побудуванні загальних параметрів цифрового підпису, обчисленні цифрового підпису, а також для побудови відкритих і особистих ключів цифрового підпису будемо використовувати генератор випадкових послідовностей, визначений у додатку А ДСТУ4145-2002 [15].

Розглянемо схему ЦП у вигляді чотирьох процесів [254]: ініціалізація, генерування асиметричної пари «особистий – відкритий ключ», підписування та перевіряння. Схема алгоритму вироблення ЦП наведена на рис. 13.3.

На етапі ініціалізації уповноважений на генерацію виробляє пару «відкритий – особистий майстер-ключ центру», тобто генерує випадкове число s' та обчислює $P_{pub} = sP$.

Якщо ID – ідентифікатор підписувача, то процес генерування асиметричної пари ключа зводиться до таких обчислень:

$$Q_{id} = H_1(ID), \tag{13.29}$$

$$d_{id} = s\,Q_{id}, \tag{13.30}$$

де d_{ID} – особистий ключ користувача,

Q_{ID} – відкритий ключ користувача,

s – особистий майстер-ключ уповноваженого на генерацію.

За аналогією з ДСТУ 4145-2002 при формуванні цифрового підпису будемо використовувати цифровий передпідпис. Для обчислення цифрового передпідпису спочатку генерується ціле число e – таке, що $0 < e < n$. Потім обчислюється відкритий ключ сеансу, тобто $Q - eP$ та $R = e(P, Q)$. Цифровим передпідписом буде значення $F_e = H_3(R)$.

Вироблення ЦП

Безпосередньо обчислення ЦП S зводиться до знаходження:

$$S = Q + H_2(M)\,H_3(R)\,d_{id}. \tag{13.31}$$

Цифровим підписом повідомлення M є пара значень (r, s).

Перевіряння ЦП

При перевірянні ЦП перевірник повинен знати загальні параметри, відкритий ключ підписувача, відкритий майстер-ключ та саме підписане повідомлення $\{M, (r, s)\}$.

Тоді двійкове подання цифрового підпису подається у вигляді двох елементів згідно формату ЕЦП. Також обчислюється значення

$$R' = e(P, s)\,e(P_{pub}, H_2(R)\,H_3(R)\,Q_{ID}). \tag{13.32}$$

Якщо $R = R'$, тоді підпис визнається дійсним, інакше – підпис недійсний.

Схема ЕЦП на основі стандарту ДСТУ 4145-2002 з використанням спарювань зображена на рис. 13.4–13.5.

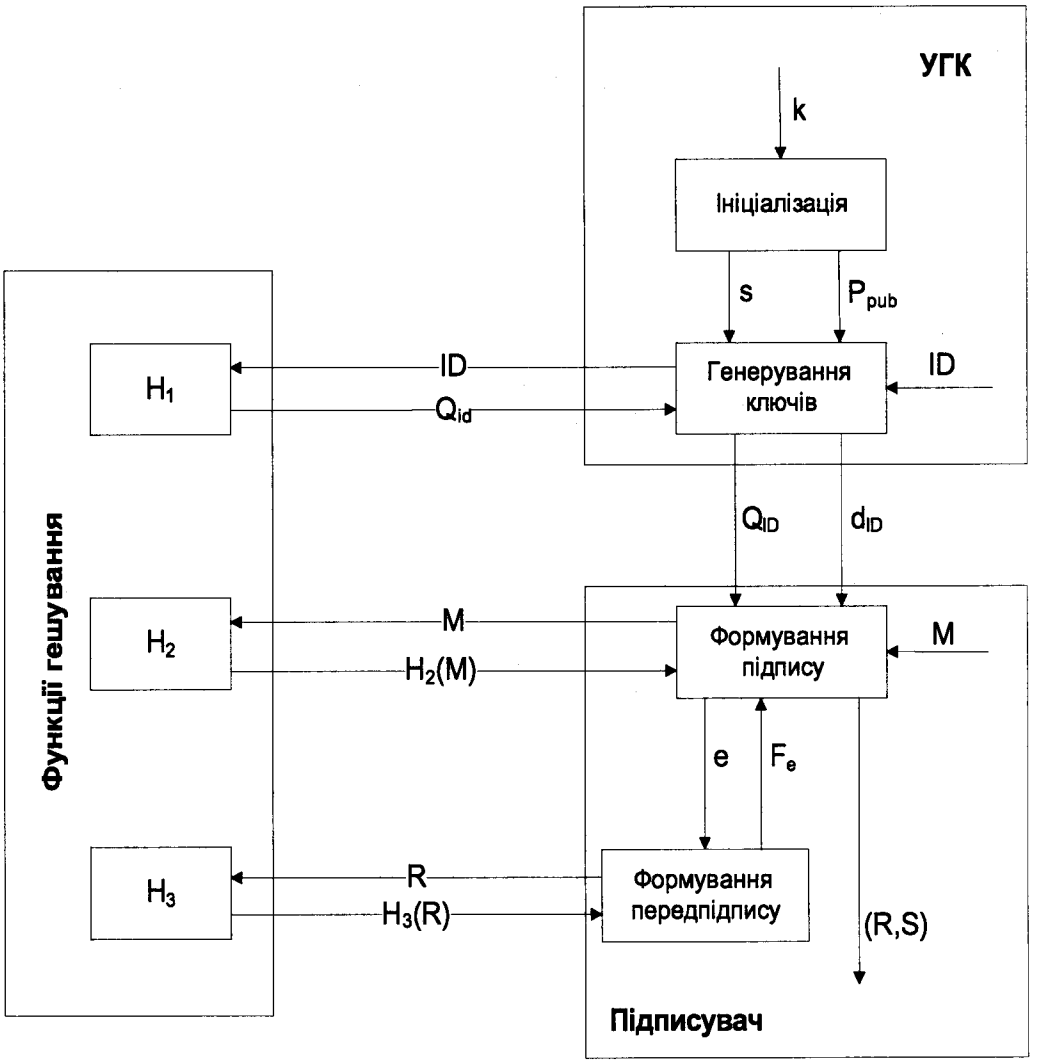

Рис. 13.4. Схема алгоритму формування ЕЦП на основі ДСТУ 4145-2002 зі спарюванням

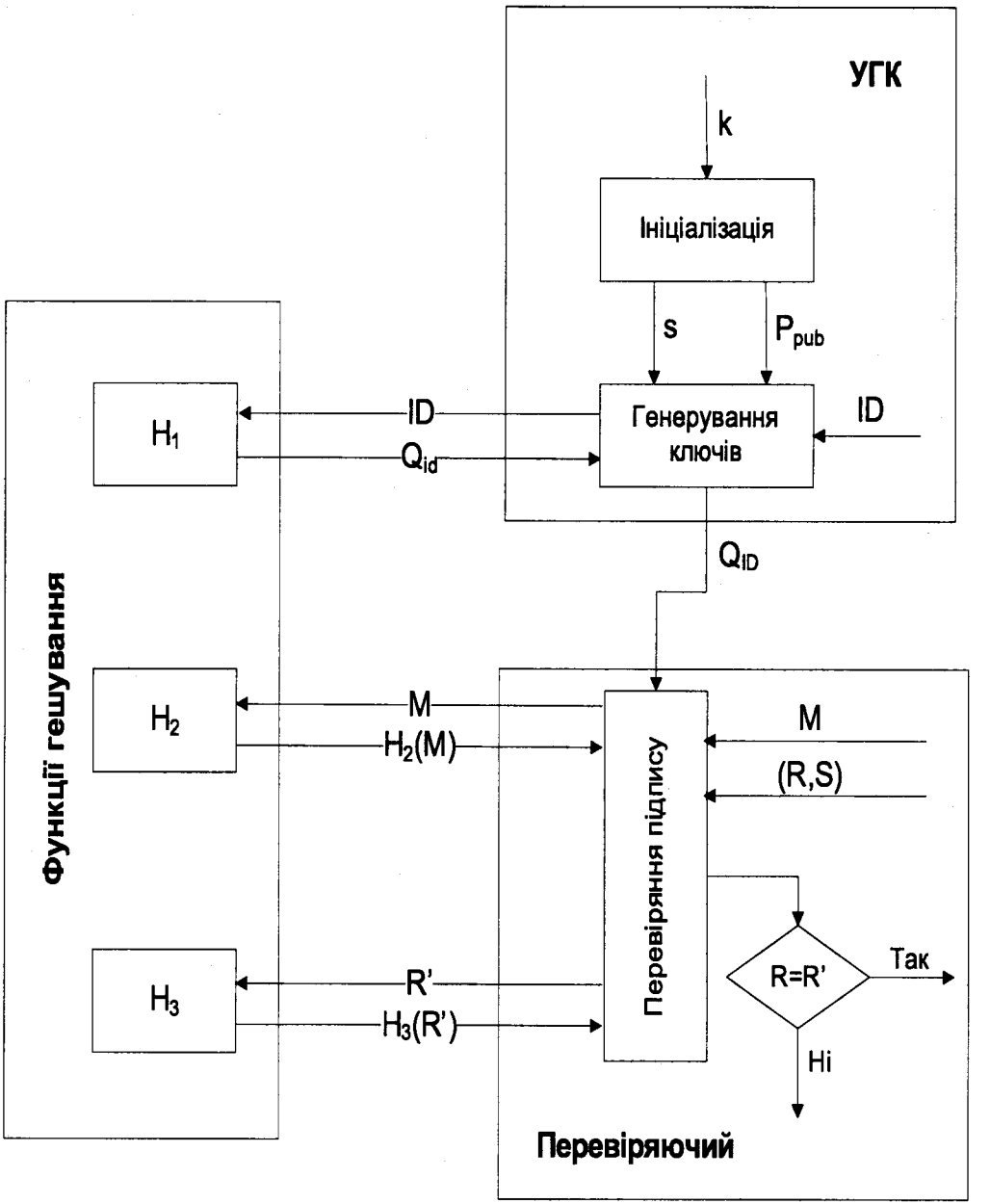

Рис. 13.5. Схема перевіряння ЕЦП на основі ДСТУ 4145-2002 з використанням парних відображень

Доведемо правильність алгоритму перевіряння цифрового підпису. Основне криптографічне перетворення при обчисленні цифрового підпису виконується над елементом $H_2(M)$ основного поля. Якщо отримане повідомлення ідентичне оригінальному, то під час перевіряння підпису буде обчислено такий самий елемент основного поля. Якщо цифровий підпис прийнято без спотворень, то для перевіряння цифрового підпису буде використана та сама пара (r, s), що була отримана під час обчислення цифрового підпису. Під час перевіряння обчислюють число R, а саме:

$$R = e(P, S)\, e(P_{pub}, H_2(M) H_3(R) Q_{ID}) =$$
$$= e(P, S)\, e(sP, H_2(M) H_3(R) Q_{ID}) = e(P, S)\, e(P, -H_2(M) H_3(R) d_{ID}) =$$
$$= e(P, H_2(M) H_3(R) d_{ID})\, e(P, Q)\, e(P, -H_2(M) H_3(R) d_{ID}) = e(P, Q).$$

По суті, доведено таке твердження.

Твердження 3.4. Алгоритм обчислення цифрового підпису згідно схем, зображених на рис. 13.4 та 13.5 коректний і задовольняє вимогам, які пред'являються до ЕЦП з додатком [254].

Опишемо обчислювальну складність алгоритмів формування та перевіряння ЕЦП, що наведено у схемах 3.4 та 3.5. Алгоритм формування потребує обчислення двох геш-значень, одного парного відображення, одного множення в розширеному полі характеристики 2, двох множень точки еліптичної кривої на скаляр та одного складання у групі G_1. Тобто, отримаємо формулу складності обчислення цифрового підпису:

$$\sum_{підп} = 1M_F + 2H + 1P + 2M_E + 1A,$$

де M_F – операція множення в полі F_2^m;
H – операція отримання геш-значення;
P – функція обчислення парного відображення;
M_E – множення на скаляр у групі точок еліптичної кривої $E(F_2^m)$;
A – операція додавання у групі G_1.

Алгоритм перевірки потребує двох обчислень геш-значень, двох спарювань, одного множення в полі F_2^m та одного експоненціювання у скінченому полі, тобто

$$\sum_{перевір} = 1M_F + 2H + 2P + 1E_F, \qquad (13.33)$$

де M_F – операція множення в полі F_2^m;
H – операція отримання геш-значення;
P – функція обчислення парного відображення;
E_F – експоненціювання в групі G_2.

Зважаючи на формули (13.6) та (13.7), практично цікавим є порівняння ЕЦП згідно зі стандартом ДСТУ 4145-2002 та аналогом такого ЕЦП з використанням білінійних відображень, що наведено в табл. 13.2.

Зауважимо, що A_E – це операція додавання в групі точок ЕК, а A_F – операція додавання в скінченному полі.

Таблиця 13.2. **Порівняльний аналіз складності криптоперетворень в ЕЦП**

Схема ЕЦП	Підписування	Перевіряння
ЕЦП, що пропонується	$1M_F + 2H + 1P + 2M_E + 1A_E$	$1M_F + 2H + 2P + 1E_F$
ЕЦП згідно ДСТУ 4145-2002	$2M_F + 1H + 2M_E + 1A_F$	$2M_E + 1M_F + 1H + 1A_F$

Згідно з табл. 13.2 ЕЦП з використанням білінійних відображень на основі ДСТУ 4145-2002 має більше операцій, тобто більшу складність криптоперетворень. Але, враховуючи те, що функції гешування мають невеликий вплив на оцінку складності криптоперетворень у порівнянні з операціями в групі точок ЕК, можливість попереднього обчислення спарювання точок у цифровому передпідпису, а також відсутність множення на скаляр у процедурі перевіряння, можна зробити висновок, що ЕЦП з використанням білінійних відображень на основі ДСТУ 4145-2002 наближена до часових характеристик національної схеми ЕЦП.

13.8. БЕЗПЕЧНИЙ ПРОТОКОЛ РОЗДІЛЕННЯ ТАЄМНИЦІ НА ІДЕНТИФІКАТОРАХ

Сакаі, Огіші та Касахари [258, 63, 260] запропонували протокол розподілення таємниці що ґрунтується на використанні ідентифікаторів і спарюванні еліптичних кривих. Як і в криптографічних перетвореннях типу «Направлене шифрування» та «Цифровий підпис» у протоколі використовується третя довірча сторона – уповноважений на генерування ключів.

Можна виділити три основних етапи такого протоколу розподілення таємниці:

– вироблення та встановлення загальних параметрів;

– генерування ключів суб'єктів розподілення таємниці;

– розділення таємниці з використанням ідентифікаторів та спарювання точок еліптичних кривих.

На етапі вироблення та встановлення загальних параметрів виробляються або обчислюються загальні параметри аналогічно як і для цифрового підпису:

$$Params = (G_1, G_2, \ell, P, Q_B). \qquad (13.34)$$

Указані загальні параметри повинні бути розподілені між сторонами та встановлені із забезпеченням їх цілісності, справжності та доступності. На цьому етапі також обчислюється та встановлюється відкритий ключ уповноваженого на генерацію Q_{id} (головний ключ).

При цьому генерування особистих ключів користувачів здійснюється уповноваженим на генерацію. Особистий ключ d_{id} кожного користувача обчислюється уповноваженим на генерацію з використанням його особистого ключа S та відкритого ідентифікатора Q_{id} за правилом:

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

Що стосується відкритого ідентифікатора Q_{id} та особистого ключа d_{id} відповідного користувача, мають бути забезпечені цілісність, справжність, доступність і неспростовність, а щодо особистого ще додатково й високого рівня конфіденційність. Також особистий ключ потрібно передавати тільки його власникові по надійно захищеному каналу. Для цього всі користувачі повинні мати з уповноваженим на генерацію виділений захищений канал зв'язку на індивідуальних ключах.

Розділення таємниці між користувачами здійснюється з використанням особистого ключа користувача, що генерований уповноваженим на генерацію, та відкритого ключа іншого користувача (ідентифікатора ID чи Q_{id}).

Розглянемо дії уповноваженого на етапі вироблення та встановлення загальних параметрів.

По-перше, уповноважений повинен виробити або обчислити та встановити загальні параметри, забезпечивши їх цілісність, справжність і доступність. Для цього генеруються загальні параметри еліптичної кривої та поля Галуа, тобто адитивна група $(G_1, +)$ та мультиплікативна група $(G_2, \cdot)$ Указані групи повинні мати простий порядок n. Вибраний елемент, що породжує адитивну підгрупу (базова точка), $P \in G_1$. Спарювання може виконуватись з використанням звичайного чи модифікованого перетворення Вейля. Наприклад, при використанні модифікованого спарювання маємо:

$$\ell : (G_1, +)^2 \Rightarrow (G_2, \cdot).$$

Далі генерується випадкове чи псевдовипадкове число, що приймається як особистий ключ d_y уповноваженого та обчислюється відкритий ключ уповноваженого

$$Q_y = d_y P. \tag{13.35}$$

Уповноважений також повинен вибрати й узгодити стійку функцію гешування:

$$F : \{0,1\}^* \Rightarrow G_1. \tag{13.36}$$

Функція гешування необхідна для відображення ідентифікатора користувача ID d в елемент групи G_1.

Насамкінець уповноважений робить доступними для користувачів загальні параметри

$$(\mathrm{des}q(G_1), \mathrm{des}q(G_2), e, P, Q_в, F) \tag{13.37}$$

та забезпечує їх цілісність, справжність і доступність.

13.9. ТРИСТОРОННІЙ ПРОТОКОЛ УЗГОДЖЕННЯ КЛЮЧІВ ДІФФІ-ГЕЛЛМАНА НА ІДЕНТИФІКАТОРАХ

Автор [260] застосував метод спарювання та розробив протокол тристороннього узгодження ключів за допомогою досить простого способу. Він назвав свій метод «тристороннім протоколом узгодження ключів Діффі-Геллмана». У цьому протоколі знову було використано метод спарювання Вейля, але він був не занадто зручний для реальних застосувань (у ньому необхідно було генерувати лінійно незалежні точки). Для вирішення цієї проблеми був запропонований протокол, заснований на модифікованому спарюванні Вейля.

Припустимо, що A генерує компоненти свого ключа P_A:

$$P_A \leftarrow [a]P,$$

де $P \in G_1$ – точка на суперсингулярній еліптичній кривій, що має простий порядок α, а число $a < \alpha$ – ціле. Аналогічно припустимо, що B і C обчислюють параметри своїх ключів:

$$P_B \leftarrow [b]P, P_C \leftarrow [c]P,$$

де $b < \alpha$ і $c < \alpha$. Цілі числа a, b, c є секретними ключами A, B і C відповідно.

Кожний із трьох партнерів поміщає свій параметр ключа P_A, P_B або P_C у відкритий каталог. Зробивши це, вони стають власниками загального ключа:

$$e(P_B, P_C)^a = e(P_A, P_C)^b = e(P_A, P_B)^c = e(P, P)^{abc}.$$

A обчислює загальний ключ, піднісши до степеня образ першої пари, B – другий, а C – третій.

Якби в протоколі не застосовувався метод спарювання, узгодження ключа не вдалося б провести за один сеанс.

Зрозуміло, як і протокол обміну ключами Діффі-Геллмана, ця схема не має властивості автентифікації.

13.10. СТАН СТАНДАРТИЗАЦІЇ ІВК, ЩО ҐРУНТУЮТЬСЯ НА ВИКОРИСТАННІ ІДЕНТИФІКАТОРІВ

Проведений аналіз дозволяє зробити висновок, що процеси стандартизації ІВК на ідентифікаторах тільки розпочинаються. На наш погляд, першим, який можна назвати основоположним, стандартом у галузі криптографічних систем на ідентифікаторах є проект стандарту IEEE P1363.3 [248] – Draft Standard for Identity-based Public-key Cryptography Using Pairings – Проект стандарту для криптографії відкритого ключа, заснованої на ідентифікаторах, що використовує спарювання точок ЕК. Цей проект призначений для локальних мереж 802.1–802.12 і розроблений робочими групами проекту 802 Інституту Інженерів з Електротехніки Радіоелектроніки (IEEE).

У проекті стандарту IEEE P1636.3 визначені загальні методи криптографічних перетворень на ідентифікаторах, які використовують спарювання точок ЕК, включаючи секретні ключі, шифрування на відкритому ключі, цифрові підписи,

а також схеми шифрування, що засновані на цих примітивах. У стандарті також визначаються алгоритми дозволених функцій гешування, зв'язані параметри шифрування, а також відкриті та секретні ключі.

У стандарті наводиться така загальна модель побудови IBE-схем, заснованих на спарюванні точок ЕК, у тому числі:

1) базові математичні операції (примітиви), що засновані на спарюванні типу Діффі-Геллмана, на сліпих комутативних спарюваннях, а також на спарюваннях повного геш-значення домену;

2) операції, що дозволяють комбінувати примітиви та додаткові методи перетворень (шифрування, інкапсуляція ключа та підписи, що засновані на ідентифікаторах);

3) протоколи, що повинні виконуватися декількома сторонами для досягнення деякого заданого рівня безпечності.

Кожний примітив може виконувати такі функції, як генерація ключів, перевірка згенерованого значення, зашифрування та розшифрування.

Основними технічними специфікаціями, що визначають вимоги до реалізації криптографічних систем на ідентифікаторах є Internet-рекомендації RFC 5408-2009 та RFC 5091-2007 [259, 249]. Іноді вказані рекомендації називають Internet-стандартами.

Технічні специфікації RFC 5408 – Identity-Based Encryption Architecture and Supporting Data Structures (Архітектура криптографічних перетворень, що заснована на ідентифікаторах, та підтримуючі структури даних) містять опис архітектури безпеки, яка повинна бути реалізована для здійснення шифрування, заснованого на ідентифікаторах, а також технологію шифрування ключа, що використовує ідентифікатор як відкритий ключ. У рекомендаціях також визначені структури даних, які можуть бути використані для здійснення технології шифрування.

Технічні специфікації RFC 5091 [249] – Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems (Стандарт криптографічних перетворень, заснованих на ідентифікаторах: Подання на суперсингулярній еліптичній кривій криптосистем BF та BB1) містить набір специфікацій для реалізації IBE-систем перетворення (кодування), заснованих на спарюваннях. У ньому описується дві криптосистеми: система IBE, що розроблена Boneh і Franklin (BF), а також система IBE, що розроблена Boneh і Boyen (BB1). Також наводяться приклади захищених практичних реалізацій кожної із систем, у яких застосовуються основні алгоритми IBE, з рівнем безпечності, що зазвичай досягається в гібридних схемах.

У проекті стандарту примітиви подаються у вигляді математичних операцій, що використовуються як стандартні модулі.

Припускається, що примітиви задовольняють певним припущенням, які перераховані в специфікації до кожного примітиву. Якщо вхідні дані не задовольняють вимогам, то може повертатись стан «помилка», може повертатися підпис з помилкою. Наприклад, у результаті виконання підпису з використанням примітиву може повернутись щось схоже на підпис, навіть якщо на його вході не було дійсного секретного (особистого ключа), або звертання може бути відхилено. Кожне звертання повинне задовольняти прийнятим обмеженням.

Кожний із цих примітивних типів має чотири складові:

1) генерація – зазвичай використовується для витягання секретного ключа в ключовому сервері;

2) перевірка згенерованого значення;

3) шифрування;

4) дешифрування.

Стандарт IEEE P1636.3 стандартизує три типи примітивів, серед яких математичні, примітиви геш-функцій та криптографічні примітиви.

Стандартом IEEE P1636.3 рекомендовано до застосування три типи функцій гешування:

1) до цілого числа – IHF1-SHA;

2) до рядка – SHF1-SHA;

3) до точки на кривій – PHF1-SHA.

Функція IHF1-SHA ґрунтується на використанні сімейства SHA-1 та SHA-2 функцій гешування. Інші геш-функції можуть бути сконструйовані за потребою за допомогою використання IHF1-SHA [259].