ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології.
Криптографічний захист інформації.
Цифровий підпис, що ґрунтується
на еліптичних кривих.
Формування та перевірка

ДСТУ 4145 - 2002

Видання офіційне

КИЇВ
ДЕРЖСТАНДАРТ УКРАЇНИ
2003

ПЕРЕДМОВА

1 РОЗРОБЛЕНО
Малим підприємством “Дина”

ВНЕСЕНО
Департаментом спеціальних телекомунікаційних систем та захисту інформації СБ України

2 ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
наказом Держстандарту України від .....

3 ВВЕДЕНО ВПЕРШЕ

4 РОЗРОБНИКИ:
О. Шаталов (керівник розробки)
А. Кочубінський, кандидат фізико-математичних наук

ЗМІСТ

ВСТУП

Необхідність забезпечення надійного функціонування комп'ютеризованих систем оброблення інформації ставить високі вимоги щодо цілісності та автентичності даних, які надходять, зберігаються та обробляються в цих системах. Автентифікація є процедура, яка встановлює достовірність твердження, що об'єкт (чи суб'єкт) має очікувані властивості. Зокрема, автентифікація повідомлення - перевірка того, що повідомлення було передано без порушення цілісності з очікуваного джерела. Автентифікація здійснюється, виходячи з аналізу структури відповідних даних, за узгодженими алгоритмами.

Одним з найефективніших та найнадійніших підходів, які застосовуються для розв'язку задач, пов'язаних з автентифікацією даних та джерел повідомлень, є процедури цифрового підписування, побудовані на основі асиметричних криптографічних алгоритмів.

Цифровий підпис повідомлення – це блок даних невеликого розміру, одержаний в результаті криптографічного перетворення повідомлення довільної довжини з використанням особистого (таємного) ключа відправника. Процедура обчислення цифрового підпису побудована таким чином, що кожний цифровий підпис має унікальну структуру, пов'язану з повідомленням та ідентифікаційними даними власника особистого ключа. Перевірка цифрового підпису полягає в установленні істинності деяких алгебричних співвідношень між цифровим підписом та величинами, обчисленими за повідомленням, виходячи із зв'язку між відкритим та особистим ключами. Цей зв'язок не дає змоги відновити особистий ключ з відкритого. Таким чином, відкритий ключ є унікальний параметр, що дає змогу здійснити перевірку цифрового підпису конкретної особи. Унікальність цифрового підпису і відкритого ключа означає, що обчислювально неможливо визначити особистий ключ цифрового підпису за доступними даними й обчислювально неможливо знайти два повідомлення з однаковим цифровим підписом.

Цифровий підпис забезпечує автентичність повідомлення та неспростовність застосування особистого ключа (автентифікація власника цифрового підпису).

Цей стандарт установлює механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$, та правила застосування цього механізму до повідомлень, які пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення.

ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка

Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка

Information Technology. Cryptographic Techniques. Digital Signatures Based on Elliptic Curves. Generation and verification

---

Чинний від

1 ГАЛУЗЬ ВИКОРИСТАННЯ

Цей стандарт установлює механізм цифрового підписування, оснований на властивостях груп точок еліптичних кривих над полями $GF(2^m)$, та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті є посилання на такі стандарти:

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ 34.311-95 Информационная технология. Криптографическая функция хеширования.

3 ВИЗНАЧЕННЯ

Нижче подано визначення термінів, використаних у цьому стандарті.

3.1 двійковий рядок

en bit string [19]; fr ligne binaire [20]; ru двоичная строка [18]

Послідовність символів 0 і 1.

3.2 довжина двійкового рядка

en bit string length [19]; fr longueur d'une ligne binaire [20]; ru длина двоичной строки [18]

Кількість символів, що складають двійковий рядок.

3.3 конкатенація двійкових рядків

en concatenation [19], fr concaténation [20], ru конкатенация [18]

Конкатенація S||R двійкових рядків S та R є двійковий рядок, що утворюється з двійкового рядка S дописуванням до нього справа двійкового рядка R.

3.4 повідомлення T

en message [19]; fr message [20]; ru сообщение [18]

Двійковий рядок довільної довжини L_T.

3.5 функція гешування H ; геш-функція

en hash function [19]; fr fonction de hachage [20]; ru функция хеширования [18]

Криптографічне перетворення повідомлення T довільної довжини у двійковий рядок $H(T)$ фіксованої довжини L_H. Двійковий рядок $H(T)$ називається результатом гешування або геш-кодом. Алгоритм обчислення конкретної функції гешування може накладати обмеження на допустиму довжину повідомлення L_T. Значення параметра L_H визначається конкретним алгоритмом обчислення функції гешування.

3.6 випадковий двійковий рядок

en random bit string [19]; fr ligne binaire aléatoire [20]; ru случайная двоичная строка [18]

Двійковий рядок, отриманий в результаті декількох звернень до генератора випадкових послідовностей, використання якого дозволено цим стандартом.

3.7 цифровий підпис

en digital signature [19]; fr signature numérique [20]; ru цифровая подпись [18]

Двійковий рядок D довжини L_D, обчислений за правилами, встановленими цим стандартом. Довжина L_D цифрового підпису визначається, виходячи з конкретних умов реалізації цього стандарту.

3.8 просте поле $GF(2)$

en prime field [19]; fr corps premier [20]; ru простое поле [18]

Поле, що містить два елементи: 0 і 1.

3.9 основне поле

en base field [19]; fr corps de base [20]; ru основное поле [18]

Скінченне поле $GF\left(2^m\right)$, яке є розширенням степеня m поля $GF(2)$. За означенням це поле має характеристику 2. Допустимі значення степеня поля m визначаються цим стандартом. Правила виконання операцій в основному полі наведено в додатку В.

3.10 слід $tr(x)$ елемента x основного поля

en trace [19]; fr trace [20]; ru след [18]

Значення виразу $tr(x)=\sum_{i=0}^{m-1} x^{2^i}$.

Слід елемента завжди дорівнює 0 або 1 і є елементом поля $GF(2)$. Слід нульового елемента основного поля завжди дорівнює 0. Слід одиничного елемента основного поля дорівнює 1, тоді і тільки тоді, коли степінь основного поля m – непарне число.

3.11 напівслід $htr(x)$ елемента x основного поля непарного степеня m

en half trace [19]; fr demi-trace [20]; ru полуслед [18]

Елемент основного поля, який обчислюється за формулою

$$htr(x)=\sum_{i=0}^{(m-1)/2} x^{4^i}$$

3.12 порядок елемента $x\neq 0$ основного поля

en element order [19]; fr ordre d'un élément [20]; ru порядок элемента [18]

Найменше натуральне число k, таке що $x^k=1$.

3.13 примітивний елемент основного поля

en primitive element [19]; fr élément primitif [20]; ru примитивный элемент [18]

Елемент основного поля $GF\left(2^m\right)$, порядок якого дорівнює 2^m-1.

3.14 многочлен $f(t)$ степеня m над полем $GF(2)$

en polynomial [19]; fr polynôme [20]; ru многочлен [18]

Многочлен

$$f(t)=t^m+f_{m-1}t^{m-1}+\cdots+f_0,$$

де коефіцієнти многочлена $f_i\in GF(2),\quad i=0,\ldots,m-1.$

3.15 незвідний многочлен над полем $GF(2)$

en irreducible polynomial [19]; fr polynôme irréductible [20]; ru неприводимый многочлен [18]

Многочлен ненульового степеня, що ділиться над полем $GF(2)$ без залишку тільки на самого себе і многочлени нульового степеня.

3.16 корінь многочлена $f(t)$

en root of a polynomial [19]; fr racine d'un polynôme [20]; ru корень многочлена [18]

Елемент x основного поля, такий що $f(x)=0.$

3.17 примітивний многочлен

en primitive polynomial [19]; fr polynôme primitif [20]; ru примитивный многочлен [18]

Незвідний многочлен, корені якого є примітивними елементами.

3.18 примітивний тричлен

en primitive trinomial [19]; fr trinôme primitif [20]; ru примитивный трехчлен [18]

Примітивний многочлен виду

$$f(t)=t^m+t^k+1,\ 0<k<m.$$

3.19 примітивний п'ятичлен

en primitive pentanomial [19]; fr pentanôme primitif [20]; ru примитивный пятичлен [18]

Примітивний многочлен виду

$$f(t)=t^m+t^l+t^j+t^k+1,\ 0<k<j<l<m.$$

3.20 поліноміальний базис основного поля

en polynomial basis [19]; fr base polynomiale [20]; ru полиномиальный базис [18]

Базис основного поля, утворений елементами $\left(x^{m-1},\ldots,x,1\right)$ основного поля, де x – корінь примітивного многочлена $f(t)$. Поліноміальний базис у цьому стандарті задається примітивним тричленом або п'ятичленом і коренем x.

3.21 нормальний базис основного поля

en normal basis [19]; fr base normale [20]; ru нормальный базис [18]

Базис основного поля $\left(x,x^2,\ldots,x^{2^{m-1}}\right)$, утворений належно вибраним елементом x основного поля.

3.22 гаусівський оптимальний нормальний базис типу 2; оптимальний нормальний базис

en Gaussian optimal normal basis [19]; fr base normale gaussienne optimale [20]; ru гауссовский оптимальный нормальный базис [18]

Нормальний базис, такий що число $p'=2m+1$ – просте і для найменшого натурального числа k, такого що $2^k\equiv 1 \bmod (p')$, виконується одна з наступних умов:

а) $p'=1 \bmod 4$ і $k=2m$;

б) $p'=3 \bmod 4$ і $k=m$.

Значення m, що гарантують існування оптимального нормального базису, визначаються цим стандартом окремо.

3.23 еліптична крива над основним полем

en elliptic curve [19]; fr courbe elliptique [20]; ru эллиптическая кривая [18]

Множина пар (x, y) елементів основного поля, які задовольняють наступне (афінне) рівняння еліптичної кривої

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in GF(2^m), \quad B \neq 0, \quad A \in \{0,1\}$,

разом із приєднаною нескінченно віддаленою точкою O.

3.24 точка еліптичної кривої

en elliptic curve point [19]; fr point d'une courbe elliptique [20]; ru точка эллиптической кривой [18]

Пара (x, y) елементів основного поля, що задовольняють рівняння еліптичної кривої, або нескінченно віддалена точка O. Координати точки P еліптичної кривої позначаються (x_P, y_P). Нескінченно віддалена точка O не має афінних координат. Точки еліптичної кривої утворюють скінченну абелеву групу. Правила виконання операцій над точками еліптичної кривої наведено в додатку В.

3.25 порядок еліптичної кривої

en elliptic curve order [19]; fr cardinalité d'une courbe elliptique [20]; ru порядок эллиптической кривой [18]

Число точок еліптичної кривої (враховуючи і нескінченно віддалену точку).

3.26 базова точка еліптичної кривої

en elliptic curve base point [19]; fr point de base d'une courbe elliptique [20]; ru базовая точка эллиптической кривой [18]

Точка $P \neq O$ еліптичної кривої, така що $nP = O$ і $kP \neq O$, $0 < k < n$, де n є просте непарне число, яке ділить порядок еліптичної кривої. Просте число n називається порядком базової точки.

3.27 загальні параметри цифрового підпису

en digital signature domain parameters [19]; fr donnée de domaine de création de signature numérique [20]; ru общие параметры цифровой подписи [18]

Параметри цифрового підпису, що є загальними для довільного числа користувачів цифрового підпису і використовуються для обчислення й перевірки цифрового підпису відповідно до цього стандарту. Ці параметри зазвичай довгочасні. До загальних параметрів цифрового підпису належать:

- параметри основного поля $GF(2^m)$: степінь розширення m, тип базису (поліноміальний, оптимальний нормальний), якщо базис поліноміальний, то примітивний многочлен $f(t)$ (тричлен, п'ятичлен), що визначає поліноміальний базис;
- еліптична крива виду

$$y^2 + xy = x^3 + Ax^2 + B;$$

де $A, B \in GF(2^m), \quad B \neq 0, \quad A \in \{0,1\}$;

- базова точка еліптичної кривої P;
- ідентифікатор використовуваної функції гешування;
- довжина цифрового підпису L_D (довжина блоку даних, що містить цифровий підпис);

- порядок базової точки n.

Загальні параметри задаються та зображуються відповідно до цього стандарту.

3.28 особистий ключ цифрового підпису

en digital signature private key [19]; fr clef privée de signature numérique [20]; ru ключ подписи [18]

Особистий ключ цифрового підпису є індивідуальним параметром цифрового підпису, який обчислено згідно з цим стандартом.

3.29 відкритий ключ цифрового підпису

en digital signature public key [19]; fr clef publique de signature numérique [20]; ru открытый ключ цифровой подписи [18]

Точка еліптичної кривої Q, обчислена згідно з цим стандартом. Відкритий ключ цифрового підпису є індивідуальним параметром цифрового підпису. Вважається, що при перевірці підпису особа, яка перевіряє, має доступ до автентичної копії відкритого ключа.

3.30 цифровий передпідпис F_e

en digital presignature [19]; fr présignature numérique [20]; ru цифровая предподпись [18]

Елемент F_e основного поля, обчислений згідно з цим стандартом із застосуванням таємного випадкового параметра e.

4 ПОЗНАЧЕННЯ

$a \bmod b$	Ціле число, що дорівнює залишку від ділення цілого числа a на натуральне число b
$a \equiv b \bmod c$	Цілі числа a і b конгруентні за модулем натурального числа c, тобто a-b ділиться на c без залишку
$\lfloor . \rfloor$	Ціла частина виразу, що міститься в дужках, тобто найбільше ціле число, яке не перевищує значення цього виразу
$g(t) \bmod f(t)$	Залишок від ділення многочлена $g(t)$ на многочлен $f(t)$, $f(t) \neq 0$
$h(t) \equiv g(t) \bmod f(t)$	Многочлени $h(t)$ і $g(t)$ конгруентні за модулем многочлена $f(t)$, $f(t) \neq 0$,тобто многочлен $h(t)$-$g(t)$ ділиться на многочлен $f(t)$ без залишку
$L(\cdot)$	Довжина двійкового зображення цілого числа, що міститься в дужках
$\max(a,b)$	Більше з цілих чисел a і b
$\min(a,b)$	Менше з цілих чисел a і b
$\log$	Логарифм за основою 2
T	Повідомлення, для якого обчислюється цифровий підпис
L_T	Довжина повідомлення T
H	Функція гешування, геш-функція
$H(T)$	Результат обчислення функції гешування за повідомленням T (геш-код)
L_H	Довжина результату обчислення функції гешування (геш-коду)
D	Цифровий підпис

L_D	Довжина цифрового підпису, число L_D кратне 16, $L_D \geq 2L(n)$, n – порядок базової точки
$GF(2)$	Просте поле, яке складається з двох елементів 0 і 1
$GF(2^m)$	Основне поле, розширення простого поля степеня m
m	Степінь основного поля – непарне просте число, $163 \leq m \leq 509$
0	Нульовий елемент основного поля
1	Одиничний елемент основного поля
x^{-1}	Обернений елемент для елемента основного поля x, $x \neq 0$
$tr(x)$	Слід елемента основного поля x
$htr(x)$	Напівслід елемента основного поля x, m – непарне число
$f(t)$	Примітивний тричлен або п'ятичлен степеня m, який задає поліноміальний базис основного поля
(A,B)	Коефіцієнти рівняння еліптичної кривої, $A \in \{0,1\}$, $B \neq 0$
O	Нескінченно віддалена точка еліптичної кривої
P	Базова точка еліптичної кривої
(x_P, y_P)	Координати базової точки еліптичної кривої P
$\tilde{P}$	Стиснене зображення точки P, елемент основного поля
n	Порядок базової точки еліптичної кривої, просте непарне число, $n \geq \max\left(2^{160}, 4\left(\left\lfloor \sqrt{2^m} \right\rfloor + 1\right)\right)$
d	Таємний ключ цифрового підпису, ціле число, $0 < d < n$
Q	Відкритий ключ цифрового підпису, точка еліптичної кривої
(x_Q, y_Q)	Координати відкритого ключа цифрового підпису
$\tilde{Q}$	Стиснене зображення точки Q, елемент основного поля
F_t	Цифровий передпідпис $F_e \in GF(2^m)$
$a \leftarrow b$	Підставлення замість змінної a виразу b
iH	Ідентифікатор геш-функції
$S\|\|R$	Конкатенація рядків S та R

5 ЗОБРАЖЕННЯ ДАНИХ І ПЕРЕТВОРЕННЯ ДАНИХ

Цей розділ установлює формати зображення математичних об'єктів, що використовуються в цьому стандарті, і правила перетворення даних з одного типу до іншого.

5.1 Зображення цілих невід'ємних чисел

Цілі невід'ємні числа зображаються у вигляді двійкових рядків, що відповідають зображенню цих чисел у системі числення за основою 2. Таким чином, якщо a – натуральне число і

$$a = \sum_{i=0}^{L-1} a_i 2^i,\ a_{L-1} = 1,\ \ a_i \in \{0,1\}\ ,$$

то це число a зображується двійковим рядком $(a_{L-1},\ldots,a_0)$. Крайній правий символ у цьому зображенні відповідає наймолодшому розряду цілого числа, крайній лівий розряд завжди дорівнює одиниці і відповідає найстаршому розряду цілого числа. Довжиною зображення натурального числа a називається натуральне число $L=L(a)$, яке обчислюється за формулою

$$L(a) = \lfloor \log a \rfloor + 1$$

Число 0 зображається символом 0 і довжина його зображення дорівнює 1.

5.2 Зображення основного поля

Основне поле $GF(2^m)$ зображується набором чотирьох цілих чисел (m,k,j,l). Число m позначає степінь розширення простого поля. Числа (l,j,k) – параметри, відповідно до розділу 3, примітивного многочлена $f(t)$, що задає поліноміальний базис. Якщо $f(t)$ - тричлен, то $k>0$, $j=l=0$. Якщо $f(t)$ – п'ятичлен, то всі числа l,j,k додатні. Якщо використовується оптимальний нормальний базис, то $l=j=k=0$.

5.3 Зображення елементів основного поля

Елементи основного поля $GF(2^m)$ зображаються двійковими рядками довжини m. Таким чином, якщо $x \in GF(2^m)$, то $x=(x_{m-1},\ldots,x_0)$, x_i дорівнює 0 або 1 для всіх значень індексу i. Якщо основне поле задано поліноміальним базисом, то крайній правий елемент зображення елемента основного поля відповідає елементу базису 1, а крайній лівий елемент зображення відповідає елементу базису x^{m-1}. Зображення елемента основного поля залежить від примітивного многочлена, що задає поле. Якщо основне поле задано оптимальним нормальним базисом, то крайній правий елемент зображення відповідає елементу нормального базису $x^{2^{m-1}}$, а крайній лівий елемент зображення відповідає елементу базису x. Нульовий елемент 0 основного поля зображається двійковим рядком, який складається з m нулів незалежно від використовуваного базису. Дозволяється зображувати нульовий елемент поля цілим числом 0. Одиничний елемент 1 основного поля зображається в поліноміальному базисі двійковим рядком, крайній правий елемент якого дорівнює 1, а решта елементів зображення дорівнюють 0. В оптимальному нормальному базисі одиничний елемент 1 зображається двійковим рядком, що складається з m одиниць. Дозволяється зображувати одиничний елемент поля цілим числом 1.

5.4 Зображення еліптичної кривої

Еліптична крива

$$y^2 + xy = x^3 + Ax^2 + B\ ,$$

де $A,B \in GF(2^m),\quad B \neq 0,\quad \mathrm{A} \in \{0,1\}$

зображається парою коефіцієнтів (A,B). Коефіцієнти еліптичної кривої зображаються згідно з 5.3.

5.5 Зображення точок еліптичної кривої

Точка еліптичної кривої $P \neq O$ зображається парою афінних координат (x_P, y_P), $x_P, y_P \in GF(2^m)$. Координати точки еліптичної кривої зображаються згідно з 5.3.

Нульовий елемент групи точок еліптичної кривої O дозволяється зображувати у вигляді пари нульових елементів основного поля: $O=(0,0)$.

5.6 Зображення результату обчислення функції гешування (геш-коду)

Результат обчислення функції гешування зображається у вигляді двійкового рядка $(h_{L_H-1},\ldots,h_0)$, довжина якого L_H визначається конкретним алгоритмом обчислення функції гешування, що використовується сумісно з цим стандартом, зокрема, $L_H=256$, якщо використовується функція гешування, встановлена в ГОСТ 34.311.

5.7 Зображення цифрового підпису

Цифровий підпис зображається двійковим рядком виду $D=(D_{L_D-1},\ldots,D_0)$. Довжина цифрового підпису L_D є ціле число, кратне 16, яке задовольняє нерівність $L_D\geq 2L(n)$, де $L(n)$ – довжина зображення порядку базової точки еліптичної кривої. Конкретне значення довжини L_D цифрового підпису обирається користувачем, виходячи з умов реалізації цього стандарту.

5.8 Перетворення елемента основного поля на ціле число

Цей підрозділ установлює алгоритм перетворення елемента основного поля $x\in GF(2^m)$ на ціле число a.

Вхідні дані алгоритму: елемент основного поля $x\in GF(2^m)$, $x=(x_{m-1},\ldots,x_0)$ і порядок базової точки еліптичної кривої n.

Результат виконання алгоритму – ціле число $a=(a_{L-1},\ldots,a_0)$, що задовольняє умову $L=L(a)<L(n)$.

Алгоритм перетворення елемента основного поля на ціле число:

1. Якщо елемент x основного поля дорівнює 0, то $a\leftarrow 0$ $L=L(a)\leftarrow 1$, кінець алгоритму.
2. Обчислюють ціле число $k=L(n)-1$.
3. Приймають $a_i=x_i$ $i=0,\ldots,k-1$ та знаходять j, що дорівнює найбільшому індексу i, при якому $a_i=1$ Якщо такого індексу нема, то приймають $a\leftarrow 0$ та закінчують виконання алгоритму.
4. Двійковий рядок $(a_j,\ldots,a_0)$ довжини $L=L(a)=j+1$ зображує ціле число a, яке є результат виконання алгоритму.

5.9 Перетворення геш-коду на елемент основного поля

Цей підрозділ встановлює алгоритм перетворення результату обчислення функції гешування $(h_{L_H-1},\ldots,h_0)$ на елемент основного поля $x\in GF(2^m)$, $x=(x_{m-1},\ldots,x_0)$.

Вхідні дані алгоритму: геш-код $(h_{L_H-1},\ldots,h_0)$.

Результат виконання алгоритму – елемент основного поля $x\in GF(2^m)$, $x=(x_{m-1},\ldots,x_0)$.

Алгоритм перетворення результату обчислення функції гешування на елемент основного поля:

1. Обчислюють ціле число $k=\min(m,L_H)$.

2. Приймають $x_i = h_i$ для $i = 0,\ldots,k-1$.

3. Якщо $k < m$, то приймають $x_i = 0$ для $i = k,\ldots,m-1$.

4. Двійковий рядок $(x_{m-1},\ldots,x_0)$ зображує елемент x основного поля, який є результат виконання алгоритму.

5.10 Перетворення пари цілих чисел на цифровий підпис

Цей підрозділ встановлює алгоритм перетворення пари цілих чисел (r,s), які задовольняють умови $0 < r < n$, $0 < s < n$, на цифровий підпис $D = (D_{L_D-1},\ldots,D_0)$.

Вхідні дані алгоритму: пара цілих чисел (r,s) у двійковому зображенні: $r = (r_{L(r)-1},\ldots,r_0)$, $s = (s_{L(s)-1},\ldots,s_0)$, $0 < r < n$, $0 < s < n$, довжина цифрового підпису L_D: $L_D \geq 2L(n)$, L_D кратне 16.

Результат виконання алгоритму – цифровий підпис $D = (D_{L_D-1},\ldots,D_0)$ довжини L_D.

Алгоритм перетворення пари цілих чисел на цифровий підпис:

1. Приймають $l = L_D/2$;

2. Утворюють двійковий рядок R за правилом

2.1. Приймають $R_i = r_i$ для $i = 0, \ldots, L(r)-1$;

2.2. Приймають $R_i = 0$ для $i = L(r), \ldots, l-1$;

3. Утворюють двійковий рядок S за правилом

3.1. Приймають $S_i = s_i$ для $i = 0, \ldots, L(s)-1$;

3.2. Приймають $S_i = 0$ для $i = L(s), \ldots, l-1$;

4. Рядок D є конкатенація двох рядків $S||R$,

5. Двійковий рядок $D = (D_{L_D-1},\ldots,D_0)$ довжини L_D є результат виконання алгоритму.

5.11 Перетворення двійкового рядка на пару цілих чисел

Цей підрозділ встановлює алгоритм перетворення двійкового рядка D парної довжини L_D на пару цілих чисел $r = (r_{L(r)-1},\ldots,r_0)$, $s = (s_{L(s)-1},\ldots,s_0)$.

Вхідні дані алгоритму: двійковий рядок $D = (D_{L_D-1},\ldots,D_0)$ парної довжини L_D.

Результат виконання алгоритму – пара цілих чисел $r = (r_{L(r)-1},\ldots,r_0)$ і $s = (s_{L(s)-1},\ldots,s_0)$

Алгоритм перетворення двійкового рядка на пару цілих чисел:

1. Обчислюють ціле число $l = L_D/2$.

2. Приймають $r_i = D_i$ для $i = 0,\ldots,l-1$.

3. Визначають j як найбільше i, $i = 0,\ldots,l-1$, для якого $r_i = 1$.

4. Якщо такого індексу нема, то $r \leftarrow 0$, $j = 0$ та переходять до кроку 6.

5. Двійковий рядок $(r_{L(r)-1},\ldots,r_0)$, $L(r) = j+1$ зображає ціле число r.

6. Приймають $s_i = D_{i+l}$ для $i = 0,\ldots,l-1$.

7. Визначають індекс j як найбільше i, $i = 0, \ldots, l-1$, для якого $s_i = 1$.

8. Якщо такого індексу нема, то $s \leftarrow 0$, $j = 0$ та переходять до кроку 10.

9. Двійковий рядок $(s_{L(s)-1},\ldots,s_0)$, $L(s) = j+1$ зображає ціле число s.

10. Пара цілих чисел r і s є результат виконання алгоритму.

6 ОБЧИСЛЮВАЛЬНІ АЛГОРИТМИ

В цьому розділі описано правила реалізації процедур, необхідних для побудови криптографічних алгоритмів, установлених цим стандартом

6.1 Генератор випадкових послідовностей

Генератор випадкових послідовностей використовується для отримання випадкових даних, необхідних для побудови загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифрового підпису.

Як генератор випадкових послідовностей треба використовувати генератор випадкових послідовностей, визначений у додатку А, або будь-який інший генератор випадкових послідовностей, рекомендований уповноваженим виконавчим органом державної влади.

6.2 Функція гешування

У цьому стандарті функція гешування використовується для обчислення й перевірки цифрового підпису. Функція гешування H перетворює текст T довільної довжини L_T на двійковий рядок $H(T)$ фіксованої довжини L_H.

У цьому стандарті повинна використовуватися функція гешування, встановлена в ГОСТ 34.311, або будь-яка інша функція гешування, рекомендована уповноваженим виконавчим органом державної влади. Значення параметра L_H однозначно визначається ідентифікатором iH конкретної функції гешування, яка використовується сумісно з цим стандартом. Параметр iH належить до загальних параметрів цифрового підпису. Таких параметрів у групі користувачів може бути декілька. При цьому $L_H \geq 160$, $L(iH) \leq 64$. Значення $iH = 1$, $L(iH) = 8$ відповідають функції гешування, встановленій в ГОСТ 34.311. Дозволено використовувати геш-функцію за промовчанням. При цьому iH може не існувати.

Якщо використовувана функція гешування накладає обмеження на довжину L_T повідомлення, то ці обмеження мають силу і для цього стандарту.

6.3 Обчислення випадкового цілого числа

В цьому підрозділі встановлено алгоритм обчислення випадкового цілого числа a, такого що $L(a) < L(n)$. Як генератор випадкових послідовностей повинен використовуватись генератор випадкових послідовностей, визначений у 6.1.

Вхідні дані алгоритму: порядок базової точки еліптичної кривої n, довжина t випадкової послідовності, що видається генератором випадкових послідовностей за одне звернення до нього.

Результат виконання алгоритму – випадкове ціле число a, $L(a) < L(n)$.

Алгоритм обчислення випадкового цілого числа:

1. Обчислюють довжину $L(n)$ двійкового зображення цілого числа n.
2. Обчислюють мінімальне значення k, для якого $kt \geq L(n) - 1$.
3. За k звернень до генератора випадкових послідовностей формують випадковий двійковий рядок довжини kt. Перші $L(n) - 1$ елементи цієї послідовності формують випадковий двійковий рядок $R_{L(n)-2}, ..., R_0$ довжини $L(n) - 1$.
4. Приймають $a_i = R_i$ для $i = 0, \ldots, L(n) - 2$.
5. Знаходять індекс j як найбільше i, для якого $a_i = 1$, якщо такого індексу нема, то приймають $a \leftarrow 0$ та припиняють виконання алгоритму.
6. Випадковий рядок $R_{L(n)-2}, ..., R_0$ знищують.

Двійковий рядок $(a_j, \ldots . a_0)$ зображує випадкове ціле число a, яке є результат виконання алгоритму.

6.4 Обчислення випадкового елемента основного поля

В цьому підрозділі встановлено алгоритм обчислення випадкового елемента x основного поля $GF(2^m)$. Як генератор випадкових послідовностей треба використовувати генератор випадкових послідовностей, визначений у 6.1.

Вхідні дані алгоритму: степінь основного поля m, довжина t випадкової послідовності, що видається генератором випадкових послідовностей за одне звернення до нього .

Результат виконання алгоритму – випадковий елемент основного поля x.

Алгоритм обчислення випадкового елемента основного поля:

1. За k звернень до генератора випадкових послідовностей формують випадковий двійковий рядок довжини $kt \geq m$, де k - мінімальне число з такою властивістю.
2. Перші m елементів цього рядка формують випадковий двійковий рядок $(R_{m-1},\ldots,R_0)$.
3. Приймають $x_i = R_i$ для $i = 0,\ldots,m-1$.
4. Випадковий двійковий рядок $(R_{m-1},\ldots,R_0)$ знищують.
5. Двійковий рядок $(x_{m-1},\ldots.x_0)$ зображує випадковий елемент x основного поля.

6.5 Обчислення сліду елемента основного поля

У цьому підрозділі встановлено алгоритм обчислення сліду елементу x основного поля.

Вхідні дані алгоритму: елемент x основного поля $GF(2^m)$.

Результат виконання алгоритму – слід $tr(x)$ елемента x.

Алгоритм обчислення сліду:

1. Приймають $t = x$.
2. Для i від 1 до $m-1$ обчислюють $t \leftarrow t^2 + x$.
3. Результат обчислення сліду $tr(x) = t$.

6.6 Обчислення напівсліду елемента основного поля

У цьому підрозділі встановлено алгоритм обчислення напівсліду елемента x основного поля.

Вхідні дані алгоритму: елемент x основного поля $GF(2^m)$ непарного степеня m.

Результат виконання алгоритму – напівслід $htr(x)$ елемента x.

Алгоритм обчислення напівсліду:

1. Приймають $t = x$.
2. Для i від 1 до $\frac{m-1}{2}$ обчислюють $t \leftarrow t^4 + x$.
3. Результат обчислення напівсліду: $htr(x) = t$.

6.7 Розв'язання квадратного рівняння в основному полі

У цьому підрозділі встановлено алгоритм розв'язання квадратного рівняння $z^2 + uz = w$ в основному полі.

Вхідні дані алгоритму: квадратне рівняння $z^2 + uz = w$; $u, w \in GF(2^m)$; m –непарне число.

Результат виконання алгоритму – кількість розв'язків k квадратного рівняння й один з розв'язків цього рівняння, якщо $k > 0$.

Алгоритм розв'язування квадратного рівняння:

1. Якщо $u = 0$, то приймають $z = w^{2^{m-1}} = \sqrt{w}$, k=1 і переходять до кроку 8.

2. Якщо $w = 0$, то приймають z=0, k=2 , і переходять до кроку 8.

3. Обчислюють елемент основного поля $v = wu^{-2}$.

4. Обчислюють слід елемента $tr(v)$ згідно з 6.5.

5. Якщо $tr(v) = 1$, то приймають $k = 0$, $z = 0$, і переходять до кроку 8.

6. Обчислюють напівслід елемента v, $t = htr(v)$, згідно з 6.6.

7. Обчислюють елемент основного поля $z = tu$, приймають $k = 2$.

8. Результат виконання алгоритму: кількість розв'язків квадратного рівняння k та один з розв'язків z, якщо $k > 0$.

6.8 Обчислення випадкової точки еліптичної кривої

У цьому підрозділі встановлено алгоритм обчислення випадкової точки еліптичної кривої.

Вхідні дані алгоритму: еліптична крива $y^2 + xy = x^3 + Ax^2 + B$ над полем $GF(2^m)$, m - непарне число, $A \in \{0,1\}$, $B \neq 0$.

Результат виконання алгоритму – випадкова точка цієї еліптичної кривої $P = (x_P, y_P)$.

Алгоритм обчислення випадкової точки еліптичної кривої:

1. Обчислюють випадковий елемент u основного поля згідно з 6.4.

2. Обчислюють елемент основного поля $w = u^3 + Au^2 + B$.

3. Розв'язують квадратне рівняння $z^2 + uz = w$ згідно з 6.7.

4. Якщо кількість розв'язків квадратного рівняння дорівнює 0, то переходять до кроку 1, інакше переходять до кроку 5.

5. Приймають $x_P = u$, $y_P = z$, z – розв'язок квадратного рівняння, отриманий на кроці 3.

6. Результат виконання алгоритму – випадкова точка еліптичної кривої P з координатами (x_P, y_P).

6.9 Стискання точки еліптичної кривої

У цьому підрозділі встановлено алгоритм перетворення точки P непарного простого порядку еліптичної кривої над $GF(2^m)$ з координатами (x_P, y_P) у стиснене зображення $\tilde{P} \in GF(2^m)$, m – непарне число.

Вхідні дані алгоритму: точка еліптичної кривої P непарного простого порядку n з координатами (x_P, y_P).

Результат виконання алгоритму – стиснене зображення $\tilde{P} \in GF(2^m)$ точки P еліптичної кривої.

Алгоритм стискання точки еліптичної кривої:

1. Якщо $x_P = 0$, то приймають $\tilde{P} = O$ та переходять до кроку 3.

2. Якщо $x_P \neq 0$, то обчислюють елемент основного поля $y = y_P x_P^{-1} = (y_{m-1}, \ldots, y_0)$, обчислюють слід елемента y, i=tr(y) та приймають $\tilde{P} = (\tilde{P}_{m-1}, \ldots, \tilde{P}_0) = (x_{P,m-1}, \ldots, x_{P,1}, i)$, тобто крайній правий двійковий розряд координати x_P замінюють на значення сліду елемента y.

3. Результат виконання алгоритму: $\tilde{P} \in GF(2^m)$ – стиснене зображення точки P еліптичної кривої.

6.10 Відновлення точки еліптичної кривої

У цьому підрозділі встановлено алгоритм відновлення точки еліптичної кривої P з її стисненого зображення $\tilde{P}$, отриманого згідно з 6.9.

Вхідні дані алгоритму: стиснене зображення $\widetilde{P} \in GF(2^m)$ точки еліптичної кривої, коефіцієнти еліптичної кривої (A, B).

Результат виконання алгоритму – точка еліптичної кривої P з координатами (x_P, y_P).

Алгоритм відновлення точки еліптичної кривої:

1. Якщо $\widetilde{P} = 0$, то приймають $x_P = 0$, $y_P = B^{2^{m-1}} = \sqrt{B}$ та переходять до кроку 7.

2. Виділяють крайній правий двійковий розряд k стисненого зображення точки $\widetilde{P} = (\widetilde{P}_{m-1}, \ldots, \widetilde{P}_0)$: $k = \widetilde{P}_0$.

3. Координату x_P точки P еліптичної кривої приймають рівною $x_P = (x_{P,m-1}, \ldots, x_{P,1}, x_{P,0}) = \widetilde{P}$, далі крайній правий розряд приймають рівним $x_{P,0} = 0$. Якщо слід отриманої координати $tr(x_P) \neq A$, то крайній правий розряд приймають рівним $x_{P,0} = 1$.

4. Обчислюють елемент $w = x_P^3 + Ax_P^2 + B$ основного поля

5. Розв'язують квадратне рівняння $z^2 + z = v$, $v = wx_P^{-2}$, згідно з 6.7.

6. Якщо слід $tr(z)$ розв'язку $z = (z_{m-1}, \ldots, z_0)$ квадратного рівняння дорівнює k, то приймають $y_P = zx_P$, інакше приймають $y_P = (z+1)x_P$.

7. Результат виконання алгоритму – точка еліптичної кривої $P = (x_P, y_P)$.

6.11 Перевірка примітивності многочлена

У цьому підрозділі встановлено алгоритм перевірки примітивності многочлена $f(t)$ степеня m над скінченним полем $GF(2)$.

Вхідні дані алгоритму: многочлен $f(t) = t^m + f_{m-1}t^{m-1} + \cdots + f_0$, коефіцієнти якого належать до поля $GF(2)$, m – непарне число.

Результат виконання алгоритму – повідомлення "многочлен примітивний" або повідомлення "многочлен не примітивний".

Алгоритм перевірки примітивності многочлена:

1. Приймають $g(t) = t$.

2. Для i від 1 до $\left\lfloor \frac{m}{2} \right\rfloor$ виконують кроки 2.1 – 2.3.

2.1 Обчислюють многочлен $g(t) \leftarrow g(t)^2 \bmod f(t)$.

2.2 Обчислюють найбільший спільний дільник $d(t)$ многочленів $f(t)$ і $g(t)+t$.

2.3 Якщо $d(t) \neq 1$, то видають повідомлення "многочлен не примітивний" і припиняють виконання алгоритму.

3. З таблиць або за допомогою факторизації визначають прості дільники $p_1, \cdots, p_k$ числа $2^m - 1$.

4. Для i від 1 до k виконують кроки 4.1 і 4.2:

4.1 Обчислюють многочлен $d_i(t) = t^{\frac{2^m-1}{p_i}} \bmod f(t)$.

4.2 Якщо $d_i(t) = 1$, то видають повідомлення "многочлен не примітивний" і припиняють виконання алгоритму.

5. Видають повідомлення "многочлен примітивний".

6.12 Перевірка простоти порядку базової точки еліптичної кривої

У цьому підрозділі встановлено алгоритм перевірки простоти порядку базової точки еліптичної кривої.

Вхідні дані алгоритму: порядок базової точки еліптичної кривої n.

Результат виконання алгоритму – повідомлення “порядок базової точки еліптичної кривої n просте число” або “порядок базової точки еліптичної кривої n складене число”.

Алгоритм перевірки простоти порядку базової точки еліптичної кривої n:

1. Обчислюють зображення числа $n-1$ вигляду $n-1=j2^k$, де j – непарне число.

2. Для i від 1 до 50 виконують кроки 2.1 - 2.3:

2.1 Обчислюють випадкове натуральне число a, $1< a < n$. Для цього:

2.1.1 Обчислюють випадкове ціле число згідно з 6.3.

2.1.2 Якщо a=0 або a=1, то переходять до кроку 2.1.1, інакше переходять до кроку 2.2.

2.2 Обчислюють ціле число $b \equiv a^j \bmod n$;

2.3 Якщо $b \neq 1$ і $b \neq n-1$, то виконують кроки 2.3.1 - 2.3.3:

2.3.1 Приймають $l=1$.

2.3.2 Доки $l \leq k-1$ і $b \neq n-1$ виконують кроки 2.3.2.1 - 2.3.2.3:

2.3.2.1 Обчислюють $b \leftarrow b^2 \bmod n$.

2.3.2.2 Якщо $b=1$, то видають повідомлення “порядок базової точки еліптичної кривої n складене число” і припиняють виконання алгоритму.

2.3.2.3 Обчислюють $l \leftarrow l+1$.

2.3.3 Якщо $b \neq n-1$, то видають повідомлення “порядок базової точки еліптичної кривої n складене число” і припиняють виконання алгоритму.

3. Видають повідомлення “порядок базової точки еліптичної кривої n просте число”.

Додатково дозволено використовувати будь-який метод, який дає строге математичне доведення простоти порядку базової точки еліптичної кривої n, наприклад, метод сум Якобі або метод еліптичних кривих.

6.13 Перевірка виконання умови Менезеса-Окамото-Венстона

У цьому підрозділі встановлено алгоритм перевірки виконання умови Менезеса-Окамото-Венстона для порядку n базової точки еліптичної кривої.

Вхідні дані алгоритму: порядок n базової точки еліптичної кривої, визначеної над скінченним полем $GF(2^m)$.

Результат виконання алгоритму – повідомлення “умова Менезеса-Окамото-Венстона виконана” або повідомлення “умова Менезеса-Окамото-Венстона не виконана”.

Алгоритм перевірки виконання умови Менезеса-Окамото-Венстона:

1. Обчислюють ціле число $k=2^m \bmod n$.

2. Приймають $j=1$.

3. Для i від 1 до 32 виконують кроки 3.1 – 3.2:

3.1 Обчислюють нове значення цілого числа j: $j \leftarrow jk \bmod n$.

3.2 Якщо $j=1$, то видають повідомлення “умова Менезеса-Окамото-Венстона не виконана” і припиняють виконання алгоритму.

4. Видають повідомлення “умова Менезеса-Окамото-Венстона виконана”.

7 ОБЧИСЛЕННЯ ЗАГАЛЬНИХ ПАРАМЕТРІВ ЦИФРОВОГО ПІДПИСУ

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

7.1 Вибір основного поля

Дозволено задавати основне поле поліноміальним або оптимальним нормальним базисом.

Якщо використовується поліноміальний базис, то основне поле треба вибирати серед полів $GF(2^m)$, степені яких наведено в таблиці 1. Поліноміальний базис задають примітивними тричленами або примітивними п'ятичленами. Використання примітивних многочленів, наведених у таблиці 1, не є обов'язковим.

Таблиця 1 - Допустимі основні поля з поліноміальним базисом і рекомендовані примітивні многочлени

№ ч/ч	Степінь поля m	Примітивний многочлен	№ ч/ч	Степінь поля m	Примітивний многочлен
1	163	$x^{163}+x^7+x^6+x^3+1$	31	337	$x^{337}+x^{10}+x^6+x+1$
2	167	$x^{167}+x^6+1$	32	347	$x^{347}+x^{17}+x^6+x+1$
3	173	$x^{173}+x^{10}+x^2+x+1$	33	349	$x^{349}+x^6+x^5+x^2+1$
4	179	$x^{179}+x^4+x^2+x+1$	34	353	$x^{353}+x^{26}+x^7+x^3+1$
5	181	$x^{181}+x^7+x^6+x+1$	35	359	$x^{359}+x^{18}+x^4+x^2+1$
6	191	$x^{191}+x^9+1$	36	367	$x^{367}+x^{21}+1$
7	193	$x^{193}+x^{15}+1$	37	373	$x^{373}+x^9+x^6+x+1$
8	197	$x^{197}+x^{21}+x^2+x+1$	38	379	$x^{379}+x^{17}+x^6+x+1$
9	199	$x^{199}+x^{11}+x^2+x+1$	39	383	$x^{383}+x^9+x^5+x+1$
10	211	$x^{211}+x^{12}+x^6+x+1$	40	389	$x^{389}+x^{17}+x^{10}+x+1$
11	223	$x^{223}+x^{12}+x^2+x+1$	41	397	$x^{397}+x^{22}+x^3+x+1$
12	227	$x^{227}+x^{21}+x^2+x+1$	42	401	$x^{401}+x^{29}+x^4+x+1$
13	229	$x^{229}+x^{21}+x^2+x+1$	43	409	$x^{409}+x^{15}+x^6+x+1$
14	233	$x^{233}+x^9+x^4+x+1$	44	419	$x^{419}+x^{21}+x^{14}+x+1$
15	239	$x^{239}+x^{15}+x^2+x+1$	45	421	$x^{421}+x^7+x^4+x+1$
16	241	$x^{241}+x^{15}+x^4+x+1$	46	431	$x^{431}+x^5+x^3+x+1$
17	251	$x^{251}+x^{14}+x^4+x+1$	47	433	$x^{433}+x^{15}+x^5+x+1$
18	257	$x^{257}+x^{12}+1$	48	439	$x^{439}+x^8+x^3+x^2+1$
19	263	$x^{263}+x^{27}+x^2+x+1$	49	443	$x^{443}+x^{28}+x^3+x+1$
20	269	$x^{269}+x^7+x^6+x+1$	50	449	$x^{449}+x^{25}+x^5+x^3+1$
21	271	$x^{271}+x^{16}+x^3+x+1$	51	457	$x^{457}+x^{16}+1$
22	277	$x^{277}+x^{23}+x^3+x^2+1$	52	461	$x^{461}+x^{23}+x^4+x+1$
23	281	$x^{281}+x^9+x^4+x+1$	53	463	$x^{463}+x^{24}+x^3+x+1$
24	283	$x^{283}+x^{26}+x^9+x+1$	54	467	$x^{467}+x^{28}+x^3+x+1$
25	293	$x^{293}+x^{11}+x^6+x+1$	55	479	$x^{479}+x^{25}+x^6+x+1$
26	307	$x^{307}+x^8+x^4+x^2+1$	56	487	$x^{487}+x^{15}+x^2+x+1$
27	311	$x^{311}+x^{29}+x^4+x+1$	57	491	$x^{491}+x^{17}+x^6+x^2+1$
28	313	$x^{313}+x^7+x^3+x+1$	58	499	$x^{499}+x^{29}+x^6+x^2+1$
29	317	$x^{317}+x^9+x^5+x^2+1$	59	503	$x^{503}+x^3+1$
30	331	$x^{331}+x^{12}+x^5+x^2+1$	60	509	$x^{509}+x^{23}+x^3+x^2+1$

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

Таблиця 2 - Допустимі основні поля з оптимальним нормальним базисом

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

7.2 Вибір еліптичної кривої і порядку базової точки

Еліптичні криві для будь-якого з наведених у таблицях 1 і 2 основних полів і порядки базової точки, що їм відповідають, надаються у встановленому порядку уповноваженим виконавчим органом державної влади. Дозволено використовувати еліптичні криві, наведені в додатку Г.

7.3 Обчислення базової точки еліптичної кривої

Цей підрозділ встановлює алгоритм обчислення базової точки еліптичної кривої над основним полем.

Вхідні дані алгоритму: коефіцієнти еліптична кривої A, B і порядок базової точки n, обрані згідно з 7.1 і 7.2.

Результат виконання алгоритму – базова точка еліптичної кривої P.

Алгоритм обчислення базової точки:

1. Обчислюють випадкову точку *P* згідно з 6.8.
2. Обчислюють точку еліптичної кривої $R = nP$.
3. Якщо $R \neq O$, то переходять до кроку 1, інакше переходять до кроку 4.
4. Результат виконання алгоритму – базова точка P еліптичної кривої.

Базову точку задають її координатами. Допускається зберігання й передача базової точки у стисненому вигляді. Стискання базової точки виконують згідно з 6.9, відновлення базової точки виконують згідно з 6.10.

8 ПЕРЕВІРКА ПРАВИЛЬНОСТІ ЗАГАЛЬНИХ ПАРАМЕТРІВ ЦИФРОВОГО ПІДПИСУ

Висока криптографічна стійкість цифрового підпису, який встановлено цим стандартом, гарантується тільки в тому випадку, якщо загальні параметри цифрового підпису обчислені правильно, тобто строго відповідно до цього стандарту.

У цьому розділі встановлено правила та умови перевірки правильності загальних параметрів цифрового підпису.

8.1 Перевірка правильності вибору основного поля

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

1. Степінь основного поля міститься в таблиці 1.
2. Основне поле задано примітивним тричленом або примітивним п’ятичленом; перевірку примітивності многочлена виконують згідно з 6.11; цю перевірку не виконують, якщо примітивний многочлен міститься в таблиці 1.

Якщо основне поле задане оптимальним нормальним базисом, то перевіряється виконання наступної умови:

3. Степінь основного поля міститься в таблиці 2.

Якщо умови 1, 2 або 3 виконані, то основне поле обрано правильно.

Означену в цьому підрозділі перевірку можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування способи вибору та зберігання основного поля гарантують виконання умов 1, 2 або 3.

8.2 Перевірка правильності вибору рівняння еліптичної кривої і порядку базової точки

Коефіцієнти (A, B) рівняння еліптичної кривої повинні задовольняти наступні умови:

1. Коефіцієнт B належить основному полю, тобто є двійковим рядком довжини m.
2. Коефіцієнт *A* дорівнює 0 або 1.
3. Коефіцієнт $B \neq 0$.

Порядок *n* базової точки еліптичної кривої повинен задовольняти наступні умови:

4. n – просте непарне число; простота перевіряється згідно з 6.12.

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

6. $2^{mk} \neq 1 \bmod n$ для $k = 1, \ldots, 32$ (умова Менезеса-Окамото-Венстона). Ця умова перевіряється згідно з 6.13.

Якщо умови 1 - 6 виконано, то рівняння еліптичної кривої й порядок базової точки обрано правильно.

Означені в цьому підрозділі перевірки можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування способи отримання й зберігання коефіцієнтів рівняння еліптичної кривої й порядку базової точки цієї кривої гарантують виконання умов 1 - 6.

8.3 Перевірка правильності базової точки

Базова точка $P = (x_P, y_P)$ еліптичної кривої повинна задовольняти наступні умови:

1. Координати базової точки $P = (x_P, y_P)$ належать основному полю, тобто є двійковими рядками довжини m.

2. $P \neq O$.

3. Точка $P = (x_P, y_P)$ лежить на еліптичній кривій, тобто її координати задовольняють рівняння вибраної еліптичної кривої.

4. $nP=O$.

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

Означену в цьому підрозділі перевірку можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування способи обчислення й зберігання базової точки гарантують виконання умов 1 - 4.

9 ОБЧИСЛЕННЯ КЛЮЧІВ ЦИФРОВОГО ПІДПИСУ

Цей розділ встановлює порядок обчислення особистого d і відкритого Q ключів цифрового підпису.

9.1 Обчислення особистого ключа цифрового підпису

Особистий ключ d цифрового підпису обчислюють таким чином.

1. Обчислюють випадкове ціле число d згідно з 6.3.

2. Якщо $d \neq 0$, то d обирають як особистий ключ цифрового підпису. Інакше переходять до кроку 1.

Умови обчислення й зберігання особистого ключа цифрового підпису повинні унеможливлювати несанкціонований доступ до особистого ключа або його частини, а також до проміжних даних, які використовувались у процесі обчислення особистого ключа. Умови зберігання особистого ключа повинні унеможливлювати його модифікацію, знищення або підміну.

9.2 Обчислення відкритого ключа цифрового підпису

Відкритий ключ цифрового підпису обчислюють як точку еліптичної кривої виду $Q = -dP$, де P – базова точка еліптичної кривої, d – особистий ключ цифрового підпису.

Умови зберігання відкритого ключа мають унеможливлювати модифікацію або підміну відкритого ключа цифрового підпису. Припускається зберігання й передача відкритого ключа цифрового підпису у стисненому вигляді. Стискання відкритого ключа цифрового підпису виконують згідно з 6.9, відновлення відкритого ключа виконують згідно з 6.10.

10 ПЕРЕВІРКА ПРАВИЛЬНОСТІ КЛЮЧІВ ЦИФРОВОГО ПІДПИСУ

Висока криптографічна стійкість цифрового підпису, обчисленого згідно з цим стандартом, гарантується тільки в тому випадку, якщо особистий і відкритий ключі цифрового підпису правильні, тобто обчислені строго відповідно до цього стандарту. Цей розділ встановлює правила перевірки правильності відкритого й особистого ключів цифрового підпису.

10.1 Перевірка правильності відкритого ключа цифрового підпису

Відкритий ключ Q цифрового підпису повинен задовольняти наступні умови:

1. Координати точки еліптичної кривої, що представляє відкритий ключ цифрового підпису, належать основному полю, тобто є двійковими рядками довжини m.
2. $Q \neq O$.
3. Відкритий ключ $Q = (x_Q, y_Q)$ лежить на еліптичній кривій, тобто його координати задовольняють рівняння вибраної еліптичної кривої.
4. $nQ = O$.

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

Означену в цьому підрозділі перевірку можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування способи зберігання відкритого ключа цифрового підпису унеможливлюють його підміну, модифікацію або знищення.

10.2 Перевірка правильності особистого ключа

Перевірка правильності особистого ключа виконується тільки власником особистого ключа наступним чином:

1. Обчислюють точку еліптичної кривої $Q' = -dP$, де P–базова точка еліптичної кривої, d – особистий ключ цифрового підпису.
2. Якщо $Q' = Q$, де Q – відкритий ключ цифрового підпису, то особистий ключ відповідає відкритому ключу цифрового підпису і є правильним.

Означену в цьому підрозділі перевірку можна не виконувати, якщо використані в конкретній реалізації алгоритму цифрового підписування способи зберігання особистого ключа цифрового підпису унеможливлюють його підміну, модифікацію або знищення.

11 ОБЧИСЛЕННЯ ЦИФРОВОГО ПЕРЕДПІДПИСУ

В цьому розділі встановлено алгоритм обчислення цифрового передпідпису.

Вхідні дані алгоритму: загальні параметри цифрового підпису.

Результат виконання алгоритму – цифровий передпідпис F_e, що відповідає таємному випадковому параметру e, де e – ціле число, $0 < e < n$, $F_e \in GF(2^m)$.

Алгоритм обчислення цифрового пекрепідпису:

1. Обчислюють випадкове ціле число e згідно з 6.3.
2. Обчислюють точку еліптичної кривої $R = eP = (x_R, y_R)$.
3. Якщо координата $x_R = 0$, то переходять до кроку 1, інакше приймають $F_e = x_R$ і переходять до кроку 4.
4. Результат виконання алгоритму – цифровий передпідпис F_e та таємний випадковий параметр e.

Умови обчислення й зберігання таємного параметра e мають унеможливлювати несанкціонований доступ до нього, його частин, а також до проміжних даних, які використовувались у процесі обчислення цифрового передпідпису.

Припускається попереднє обчислення довільного числа цифрових передпідписів. Умови зберігання цифрового передпідпису мають унеможливлювати його модифікацію або підміну. Після використання цифрового передпідпису його негайно знищують разом з відповідним таємним параметром e.

12 ОБЧИСЛЕННЯ ЦИФРОВОГО ПІДПИСУ

Цей розділ встановлює алгоритм обчислення цифрового підпису.

Вхідні дані алгоритму:

- загальні параметри цифрового підпису;
- особистий ключ цифрового підпису d;
- повідомлення T довжини $L_T > 0$;

- функція гешування H згідно з 6.2;
- довжина цифрового підпису L_D, що вибирається для групи користувачів, виходячи з умов конкретної реалізації алгоритму цифрового підписування, з урахуванням умов кроку 3 алгоритму, наведеному в цьому підрозділі.

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

Алгоритм цифрового підписування:

1. Перевіряють правильність загальних параметрів цифрового підпису згідно з 8.1 - 8.3. Якщо загальні параметри цифрового підпису обчислено неправильно, то обчислення цифрового пілпису припиняють. Цю перевірку не виконуєть у випадках, передбачених 8.1 - 8.3.
2. Перевіряють правильність особистого ключа цифрового підпису згідно з 10.2. Якщо особистий ключ неправильний, то обчислення цифрового підпису припиняють. Цю перевірку не виконують у випадках, передбачених 10.2.
3. Перевіряють виконання умов: L_D - число, кратне 16, $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконана, то обчислення цифрового підпису припиняють.
4. Якщо використовується ідентифікатор геш-функції iH, то перевіряють, чи цей ідентифікатор діє у відповідній групі користувачів. Якщо ні, то обчислення цифрового підпису припиняють.
5. Якщо нормативні документи, що встановлюють обчислення функції гешування, накладають обмеження на довжину повідомлення L_T, то перевіряють виконання цих обмежень. Якщо ці обмеження не виконані, або повідомлення відсутнє, або $L_T \leq 0$, то обчислення цифрового підпису припиняють.
6. За повідомленням T обчислюють функцію гешування $H(T)$.
7. Результат обчислення функції гешування $H(T)$ перетворюють на елемент основного поля h згідно з 5.9. Якщо h=0, то приймають h=1.
8. Якщо існує набір цифрових передпідписів, обчислених заздалегідь згідно з розділом 11, то беруть будь-який з них разом з відповідним таємним параметром. Інакше обчислюють цифровий передпідпис згідно з розділом 11. Нехай на цьому кроці алгоритму отримано передпідпис F_e та відповідний таємний параметр e.
9. Обчислюють елемент основного поля $y = hF_e$.
10. Елемент основного поля y перетворюють на ціле число r згідно з 5.8.
11. Якщо $r = 0$, то переходять до кроку 8, інакше переходять до кроку 12.
12. Обчислюють ціле число $s = (e + dr) \bmod n$.
13. Якщо $s = 0$, то переходять до кроку 8, інакше переходять до кроку 14.
14. Пару цілих чисел (r, s) перетворюють на цифровий підпис D довжини L_D згідно з 5.10.
15. Результат виконання алгоритму – підписане повідомлення (iH, T, D).

13 ПЕРЕВІРКА ЦИФРОВОГО ПІДПИСУ

Цей розділ встановлює алгоритм перевірки цифрового підпису.

Вхідні дані алгоритму:

- загальні параметри цифрового підпису;
- відкритий ключ цифрового підпису Q;
- підписане повідомлення (iH, T, D) довжини $L = L(iH) + L_T + L_D$;
- функція гешування H згідно з 6.2.

Результат виконання алгоритму: повідомлення “підпис дійсний” або повідомлення “підпис недійсний”.

Алгоритм перевірки цифрового підпису:

1. Якщо використовується ідентифікатор геш-функції *iH*, то перевіряють, чи діє цей ідентифікатор у відповідній групі користувачів. Якщо ні, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

2. Виходячи з *iH* (або за промовчанням) визначають L_H.

3. Перевіряють виконання умов: L_D - число, кратне 16, $L_D \geq 2L(n)$. Якщо хоча б одна з цих умов не виконана, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

4. Перевіряють правильність обчислення загальних параметрів цифрового підпису згідно з 8.1 - 8.3. Якщо загальні параметри цифрового підпису обчислено неправильно, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису. Цю перевірку не виконують у випадках, передбачених 8.1 - 8.3.

5. Перевіряють правильність відкритого ключа цифрового підпису згідно з 10.1. Якщо відкритий ключ обчислено неправильно, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису. Цю перевірку не виконують у випадках, передбачених 10.1.

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

7. За повідомленням T обчислюють функцію гешування $H(T)$.

8. Геш-код $H(T)$ перетворюють на елемент основного поля h згідно з 5.9. Якщо h=0, то приймають h=1.

9. Цифровий підпис *D* перетворюють на пару цілих чисел (r, s) згідно з 5.11.

10. Якщо умова $0 < r < n$ не виконана, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

11. Якщо умова $0 < s < n$ не виконана, то видають повідомлення “підпис недійсний” і припиняють перевірку цифрового підпису.

12. Обчислюють точку еліптичної кривої $R = sP + rQ$, $R = (x_R, y_R)$.

13. Обчислюють елемент основного поля $y = hx_R$.

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

15. Якщо $r = \tilde{r}$, то видають повідомлення “підпис дійсний”, інакше видають повідомлення “підпис недійсний”.

ДОДАТОК А
(обов'язковий)
ГЕНЕРАТОР ВИПАДКОВИХ ДВІЙКОВИХ ПОСЛІДОВНОСТЕЙ

У цьому додатку встановлено алгоритм обчислення випадкових двійкових рядків, що йменується надалі генератором випадкових послідовностей. Цей генератор повинен використовуватися для отримання випадкових цілих чисел, випадкових елементів основного поля і випадкових точок еліптичних кривих. Генератор за одне звернення до нього видає випадковий рядок довжини $t = 1$. Як криптографічне перетворення в генераторі застосовується алгоритм криптографічного перетворення згідно з ГОСТ 28147 у режимі простої заміни. Таблиця заміни і особистий ключ цього перетворення повинні відповідати ГОСТ 28147-89. Умови отримання й використання особистого ключа повинні унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення. Особистий ключ криптографічного перетворення згідно з ГОСТ 28147, що використовується в генераторі випадкових послідовностей, не можна використовувати для іншої мети.

Позначимо через $E_k(\cdot)$ шифрування двійкового рядка довжиною 64 алгоритмом ГОСТ 28147 в режимі простої заміни на ключі k довжиною 256 двійкових розрядів. Нехай s, D, I, x – двійкові рядки довжиною 64 двійкові розряди. Перед застосуванням задають початковий стан генератора випадкових послідовностей.

Встановлення початкового стану генератора випадкових послідовностей:

- Задають початкове значення s генератора. Для цього використовують фізичне джерело випадковості. Як таке джерело можна використовувати, наприклад, квантові ефекти в напівпровідниках (шумові діоди і т.п.), сигнал від мікрофонного входу з відключеним мікрофоном, часові інтервали між натисканнями на клавіші клавіатури, часові інтервали між натисканнями на клавіші миші. Початковий стан генератора є таємним. Умови отримання початкового стану генератора повинні унеможливлювати доступ до нього або його частини, модифікацію, підміну або знищення.
- Задають значення двійкового рядка D. Для цього використовують поточне значення дати і часу з точністю 64 двійкових розрядів.
- Обчислюють двійковий рядок $I = E_k(D)$.

Використання генератора випадкових послідовностей

При кожному зверненні до генератора випадкових послідовностей виконують такі обчислення (символ $\oplus$ позначає порозрядне додавання за модулем 2 двійкових рядків довжиною 64 двійкові розряди):

- $x = E_k(I \oplus s)$;
- $s = E_k(x \oplus I)$;

Випадковий двійковий рядок є двійковий рядок довжини 1, який складається з крайнього правого розряду x_0 двійкового рядка $x = (x_{63}, \ldots, x_0)$.

ДОДАТОК Б
(довідковий)
ПРИКЛАДИ ОБЧИСЛЕНЬ ЦИФРОВОГО ПІДПИСУ

У цьому додатку наведено приклади обчислення й перевірки цифрового підпису з використанням поліноміального та оптимального нормального базисів. У прикладах обчислень двійкові рядки наведено у вигляді рядків шістнадцяткових цифр: двійковий рядок у разі потреби доповнюють зліва нулями так, щоб довжина рядка стала кратною чотирьом, потім рядок ділять на групи по 4 двійкових розряди, кожну таку групу заміняють на шістнадцяткову цифру, що відповідає цій групі двійкових символів.

Б.1 Обчислення й перевірка цифрового підпису в поліноміальному базисі

Вибір загальних параметрів

Як основне поле використовують скінченне поле $GF\left(2^{163}\right)$. Елементи цього поля зображають у поліноміальному базисі, що відповідає примітивному многочлену $x^{163}+x^7+x^6+x^3+1$ (див. Таблицю 1).

Використовується еліптична крива над полем $GF\left(2^{163}\right)$ (перша еліптична крива з таблиці Г.1):

$$y^2+xy=x^3+x^2+5\text{FF6108462A2DC8210AB403925E638A19C1455D21}.$$

Порядок цієї еліптичної кривої ділиться на просте число n=4000000000000000000002BEC12BE2262D39BCF14D, яке є порядком базової точки.

Обчислення базової точки еліптичної кривої здійснюють наступним чином: обчислюємо випадкову точку еліптичної кривої

$P=\left(x_P,y_P\right)$=(72D867F93A93AC27DF9FF01AFFE74885C8C540420,
0224A9C3947852B97C5599D5F4AB81122ADC3FD9B).

Оскільки $nP=O$, то точка P – шукана базова точка еліптичної кривої.

Як особистий ключ цифрового підпису візьмемо ціле число

d =183F60FDF7951FF47D67193F8D073790C1C9B5A3E.

Обчислимо відкритий ключ цифрового підпису, що відповідає обраному особистому ключу:

$Q=-dP=\left(x_Q,y_Q\right)$=(057DE7FDE023FF929CB6AC785CE4B79CF64ABD2DA,
3E85444324BCF06AD85ABF6AD7B5F34770532B9AA).

Нехай використовується довжина цифрового підпису L_D=512.

Припустимо, що функцію гешування вибрано згідно з ГОСТ 34.311 ($iH=1$) і ця функція використовується за промовчанням. У цьому випадку $L_H=256$. За промовчанням приймемо також, що iH не передається.

Обчислення цифрового підпису

Вважаємо, що всі перевірки згідно з розділом 12 підтверджують правильність відповідних даних. Обчислимо геш-функцію за повідомленням T. Нехай результат гешування дорівнює $H(T)$=09C9C44277910C9AAEE486883A2EB95B7180166DDF73532EEB76EDAEF52247FF.

Перетворимо результат обчислення функції гешування $H(T)$ на елемент основного поля згідно з 5.9. Перетворення цього рядка на елемент основного поля полягає у виділенні з цього рядка $\min(m,L_H)$=163 молодших розрядів. У результаті перетворення отримаємо елемент основного поля

h =03A2EB95B7180166DDF73532EEB76EDAEF52247FF.

Обчислимо передпідпис F_e згідно з розділом 11. Нехай ціле число e дорівнює

e =1025E40BD97DB012B7A1D79DE8E12932D247F61C6.

Обчислимо точку eP:

$eP = (x_{eP}, y_{eP})$=(42A7D756D70E1C9BA62D2CB43707C35204EF3C67C, 5310AE5E560464A95DC80286F17EB762EC544B15B).

Тоді F_e дорівнює координаті x_{eP} цієї точки:

F_e = 42A7D756D70E1C9BA62D2CB43707C35204EF3C67C.

Обчислимо добуток елементів основного поля

$y = hF_e$=274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Перетворимо елемент основного поля y на ціле число r згідно з 5.8:

r=274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Обчислимо ціле число

$s = e + dr \bmod n$=2100D86957331832B8E8C230F5BD6A332B3615ACA.

Перетворимо пару цілих чисел (r, s) на цифровий підпис D згідно з 5.10:

D=000000000000000000000002100D86957331832B8E8C230F5BD6A332B3615ACA000000000000000000000274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Підписане повідомлення довжини $L = L_T + L_D$ має вигляд $T \,||\, D$.

Перевірка цифрового підпису

Перевіримо цифровий підпис, обчислений вище. При перевірці цифрового підпису використовують ті самі загальні параметри, обчислений вище відкритий ключ та геш-функція за промовчанням ($iH = 1, L_H = 256$, iH не передається). Вважаємо, що всі перевірки згідно з розділом 13 підтверджують правильність відповідних даних.

Перевіряють цифровий підпис:

D=000000000000000000000002100D86957331832B8E8C230F5BD6A332B3615ACA000000000000000000000274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Перевіримо довжину цифрового підпису: $L_D = 512$, тобто чи це число кратне 16 і більше подвоєної довжини двійкового зображення порядку базової точки n.

Обчислюємо $L_T = L - L_D$. Вважаємо, що підписаний текст прийнято без спотворень, тому $L_T > 0$.

Обчислюємо $H(T)$. Підписаний текст прийнято без спотворень, тому результат обчислення функції гешування є, як і при обчисленні цифрового підпису,

$H(T)$=09C9C44277910C9AAEE486883A2EB95B7180166DDF73532EEB76EDAEF52247FF.

Перетворюємо результат обчислення функції гешування на елемент основного поля згідно з 5.9:

h=03A2EB95B7180166DDF73532EEB76EDAEF52247FF.

Перетворюємо цифровий підпис на пару цілих чисел (r, s) згідно з 5.11:

r=274EA2C0CAA014A0D80A424F59ADE7A93068D08A7,

s=2100D86957331832B8E8C230F5BD6A332B3615ACA.

Переконуємося, що $0 < r < n$.

Переконуємося, що $0 < s < n$.

Обчислюємо точку еліптичної кривої

$R = sP + rQ = (x_R, y_R)$=(42A7D756D70E1C9BA62D2CB43707C35204EF3C67C, 5310AE5E560464A95DC80286F17EB762EC544B15B).

Обчислюємо елемент основного поля

$y = hx_R$=274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Перетворюємо елемент основного поля y на ціле число $\tilde{r}$ згідно з 5.8:

$\tilde{r}$ = 274EA2C0CAA014A0D80A424F59ADE7A93068D08A7.

Оскільки $r = \tilde{r}$, то підпис дійсний.

Б.2 Обчислення й перевірка цифрового підпису в оптимальному нормальному базисі

Загальні параметри цифрового підпису

Як основне поле візьмемо поле $GF(2^{173})$ в оптимальному нормальному базисі (див. таблицю 2). Нехай еліптична крива визначена рівнянням (перша еліптична крива з таблиці Г.2):

$y^2 + xy = x^3 +$ 043D7E139319F43BA00944915740E1E6651B06E278C7.

Порядок базової точки дорівнює

n =800000000000000000000189B4E67606E3825BB2831.

Як базову точку візьмемо точку

$P = (x_P, y_P)$ =(1D26E5282C2647E1B0327CB4F6087932A0A1F006A89F,

0322218E4551CF8F6E3345644A10B2408F5DF19EC2C7).

Особистий і відкритий ключі цифрового підпису оберемо наступним чином: особистий ключ

d =49FF09C848613AEA23699F78C960D5174617311ADCC,

відкритий ключ

$Q = -dP = (x_Q, y_Q)$ =(16C1FF796B32D6D2FC83CA9530B368B322F7874B2D01,

1F253334197826B6ADAE44EDEAA7EA281D1C5E597A37).

Нехай функція гешування обчислена за промовчанням згідно з ГОСТ 34.311 ($iH = 1, L_H = 256$) та при цьому прийнято, що iH передається. Нехай результат обчислення є

$H(T)$=2A681ECE118389B27A108137187EA862117EF1484289470ECAC802C5A651FD

A8.

Припустимо, що довжина цифрового підпису дорівнює найменшому припустимому значенню L_D=352.

Обчислення цифрового підпису

Вважаємо, що всі перевірки згідно з розділом 12 підтверджують правильність відповідних даних.

Обчислимо $H(T)$ і перетворимо результат обчислення на елемент основного поля h згідно з 5.9. В результаті перетворення отримаємо елемент основного поля

h =0137187EA862117EF1484289470ECAC802C5A651FDA8

Обчислимо передпідпис F_e згідно з розділом 11. Нехай ціле число e дорівнює

e =70516411E5D9886B8486ECE54A30E9403D103B95F90.

Обчислимо точку eP:

$eP = (x_{eP}, y_{eP})$=(028886EA28A7C2951FA6473EB3EBC861D3EDB1FBB031,

19059E90F7C7725079CFFE312A389B265140F5BDA493).

Тоді F_e дорівнює координаті x_{eP} цієї точки:

F_e = 028886EA28A7C2951FA6473EB3EBC861D3EDB1FBB031.

Обчислимо добуток елементів основного поля $y = hF_e$ =0477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

Перетворимо елемент основного поля y на ціле число r згідно з 5.8:

r =477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

Обчислимо ціле число

$s = e + dr \bmod n$ =472EA56AE478F95F1EC9F628FF43857E168B50FB819

Перетворимо пару цілих чисел (r, s) на цифровий підпис D згідно з 5.10:

D=0472EA56AE478F95F1EC9F628FF43857E168B50FB8190477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

Підписане повідомлення довжини $L = 8 + L_T + L_D$ має вигляд $iH \,||\, T \,||\, D$, де iH – двійковий рядок виду 00000001.

Перевірка цифрового підпису.

Перевіримо цифровий підпис, обчислений вище. Під час перевірки цифрового підпису використовують ті самі загальні параметри, обчислений вище відкритий ключ та геш-функцію за промовчанням ($iH = 1$, $L_H = 256$, iH передається). Вважаємо, що всі перевірки згідно з розділом 13 підтверджують правильність відповідних даних.

Перевіряється цифровий підпис

D=0472EA56AE478F95F1EC9F628FF43857E168B50FB8190477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

За промовчанням, перші 8 бітів повідомлення задають iH. Перевіряємо, чи геш-функція з номером 00000001 діє на даний час, та визначаємо відповідну довжину геш-коду L_H=256.

Перевіряємо довжину цифрового підпису: $L_D = 352$, тобто чи це число кратне 16 і більше подвоєної довжини двійкового зображення порядку базової точки n.

Обчислюємо $L_T = L - L_D - L(iH)$. Вважаємо, що підписаний текст прийнято без спотворень, тому $L_T > 0$.

Обчислюємо $H(T)$. Підписаний текст прийнято без спотворень, тому результат обчислення функції гешування є, як і при обчисленні цифрового підпису,

$H(T)$=2A681ECE118389B27A108137187EA862117EF1484289470ECAC802C5A651FDA8.

Перетворюємо результат обчислення на елемент h основного поля згідно з 5.9:

h=0137187EA862117EF1484289470ECAC802C5A651FDA8.

Перетворюємо цифровий підпис на пару цілих чисел (r, s) згідно з 5.11:

r=477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A,

s=472EA56AE478F95F1EC9F628FF43857E168B50FB819.

Переконуємося, що $0 < r < n$.

Переконуємося, що $0 < s < n$.

Обчислюємо точку еліптичної кривої

$R = sP + rQ = (x_R, y_R) =$

(028886EA28A7C2951FA6473EB3EBC861D3EDB1FBB031,

19059E90F7C7725079CFFE312A389B265140F5BDA493).

Обчислюємо елемент основного поля

$y = hx_R$=0477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

Перетворюємо елемент основного поля y на ціле число $\tilde{r}$ згідно з 5.8:

$\tilde{r}$ =477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.

Оскільки $r = \tilde{r}$, то підпис дійсний.

ДОДАТОК В
(довідковий)
ОСНОВНІ МАТЕМАТИЧНІ ПОНЯТТЯ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В СТАНДАРТІ

Основними математичними об'єктами, які використовуються в цьому стандарті, є скінченні поля й еліптичні криві, визначені над цими полями. У цьому додатку наведено основні відомості про ці об'єкти, необхідні для реалізації алгоритмів, описаних у цьому стандарті. Детальний виклад теорії скінченних полів подано в монографії [1]. Уперше використовувати еліптичні криві в криптографічних цілях було запропоновано в [2] і [3]. Найкращим посібником з теорії еліптичних кривих є книги Дж.Сільвермана [4] і [5]. Простіший виклад цієї теорії з описом криптографічних застосувань міститься у книгах [6] і [7]. У статті [8] пояснено принципи побудови криптографічних алгоритмів на еліптичних кривих.

В.1 Скінченні абелеві групи

Скінченна абелева група є скінченною множиною G, на якій визначено одну операцію, що співвідносить кожній парі елементів (a,b) множини G деякий елемент c цієї самої множини. Ця операція може записуватися адитивно і тоді групова операція називається додаванням, а елемент c називається сумою елементів a і b, $c=a+b$, або мультиплікативно і тоді групова операція називається множенням, а елемент c називається добутком елементів a і b, $c=ab$.

Групова операція скінченної абелевої групи за означенням має такі властивості:

- $ab=ba$ ($a+b=b+a$) (комутативність);
- $a(bc)=(ab)c$ ($a+(b+c)=(a+b)+c$) (асоціативність);
- існує єдиний елемент групи, що позначається 1 у мультиплікативному записі і 0 в адитивному записі, такий що
- $1a=a1=a$ ($0+a=a+0=a$).

Цей елемент називається нейтральним елементом групи. У мультиплікативному записі нейтральний елемент називається одиничним елементом групи, в адитивному записі він називається нульовим елементом групи.

- Для кожного елемента групи a існує єдиний обернений елемент a^{-1} (в адитивному записі єдиний протилежний елемент $-a$), такий що

$aa^{-1}=a^{-1}a=1$ ($a+(-a)=(-a)+a=0$).

Вираз $a+(-b)$ скорочено записується $a-b$ і така операція називається відніманням. Якщо n – натуральне число, то добуток n елементів a позначається a^n. За означенням $a^0=1, a^{-n}=\left(a^{-1}\right)^n$. Операція обчислення a^n називається піднесенням елемента a до степеня n. В адитивному записі групи сума n елементів a позначається na і операція обчислення цієї суми називається множенням елемента a на натуральне число n. За означенням $0a=0$, $(-n)a=n(-a)$.

Число елементів групи N називається порядком групи. Завжди $a^N=1$ ($Na=0$). Найменше натуральне число n таке, що в мультиплікативному записі $a^n=1$, а в адитивному записі $na=0$, називається порядком елемента a. Порядок елемента завжди ділить порядок групи. Елемент a порядку n породжує циклічну підгрупу H порядку n групи G вигляду

$H=\{1,a,a^2,\ldots,a^{n-1}\}$ або $H=\{0,a,2a,\ldots,(n-1)a\}$.

Елемент a називається твірним елементом циклічної групи або примітивним елементом.

Задача розв'язання рівняння виду

$b=a^k, b\in H, 0<k<n$

або

$b = ka, b \in H, 0 < k < n$

відносно k називається задачею дискретного логарифмування в групі H.

В.2 Скінченні поля

Скінченним полем (полем Галуа) називається скінченна множина F_q=$GF(q)$, що містить q елементів і в якій визначено дві операції, одна з яких записується адитивно, а інша – мультиплікативно. Відносно адитивної операції множина F_q є скінченною абелевою групою. Відносно мультиплікативної операції скінченною абелевою групою є множина ненульових елементів F_q^*. Ці дві операції пов'язані між собою відношеннями дистрибутивності: для будь-яких елементів поля x, y, z виконується $x(y+z)=xy+xz$. Число елементів поля називається порядком поля. Порядок скінченного поля завжди є степенем деякого простого числа, $q = p^m$, число m називається степенем поля, а просте число p – його характеристикою. Мультиплікативна група скінченного поля є циклічною групою порядку $p^m - 1$, її твірний елемент називається примітивним елементом поля.

У стандарті використано скінченні поля $GF(2^m)$ характеристики 2, q=2^m, степінь розширення m – просте число, $163 \le m \le 509$. *Нульовий елемент* скінченного поля позначається символом 0, о*диничний елемент* скінченного поля позначається символом 1. У полі характеристики 2 протилежним для елемента x є сам елемент x. Таким чином, у такому скінченному полі операції додавання й віднімання ідентичні.

Найпростішим скінченним полем є скінченне поле $GF(2)$, яке складається з двох елементів 0 і 1. У цьому полі операції додавання й множення виконуються наступним чином: 0+0=0, 0+1=1+0=1, 1+1=0, 0·0=1·0=0·1=0, 1·1=1. Будь-яке скінченне поле $GF(2^m)$ є m-вимірним векторним простором над полем $GF(2)$.

Многочлен $f(t)$ степеня m над полем $GF(2)$ є многочлен вигляду

$$f(t) = t^m + f_{m-1}t^{m-1} + \cdots + f_0,$$

де коефіцієнти многочлена $f_i \in GF(2),\ i = 0, \ldots m-1$.

Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами виконуються в полі $GF(2)$. Зокрема, многочлен $g(t)$ ділиться з залишком $r(t)$ на многочлен $f(t)$, $f(t) \ne 0$, якщо $g(t)=h(t)f(t)+r(t)$, де степінь многочлена $r(t)$ менша за степінь многочлена $f(t)$. Многочлен $h(t)$ називається неповною часткою. Операція обчислення залишку від ділення многочлена $g(t)$ на многочлен $f(t)$ називається зведенням многочлена $g(t)$ за модулем $f(t)$ і позначається $g(t) \bmod f(t)$. Якщо $r(t)=0$, то многочлен $g(t)$ ділиться на многочлен $f(t)$ без залишку. Многочлени $h(t)$ і $g(t)$ конгруентні за модулем многочлена $f(t)$, $f(t) \ne 0$, якщо многочлен $h(t)$-$g(t)$ ділиться на многочлен $f(t)$ без залишку, записується $h(t) \equiv g(t) \bmod f(t)$.

Многочлен $f(t)$ ненульового степеня називається *незвідним* над полем $GF(2)$, якщо він ділиться без залишку над цим полем тільки на самого себе і на многочлени нульового степеня. Елемент x скінченного поля $GF(2^m)$ називається коренем многочлена $f(t)$, якщо $f(x)=0$. Незвідний многочлен $f(t)$ називається *примітивним*, якщо його корені є примітивними елементами поля.

Примітивним тричленом називається примітивний многочлен виду

$$f(t) = t^m + t^k + 1, 0 < k < m.$$

Примітивним п'ятичленом називається примітивний многочлен виду

$$f(t) = t^m + t^l + t^j + t^k + 1, 0 < k < j < l < m.$$

Якщо x – корінь незвідного многочлена $f(t)$ степеня m, то елементи $(x^{m-1}, \ldots, 1)$ утворюють *базис* скінченного поля $GF(2^m)$ як векторного простору над полем $GF(2)$. Цей

базис називається *поліноміальним*. Будь-який елемент основного поля однозначно виражається через елементи поліноміального базису. Найзручніше поліноміальний базис задавати примітивним многочленом.

Якщо x – такий елемент основного поля $GF\left(2^m\right)$, що елементи основного поля $\left(x, x^2, \ldots, x^{2^{m-1}}\right)$ лінійно незалежні над $GF(2)$, то ці елементи утворюють базис поля $GF\left(2^m\right)$, який називається *нормальним*. Нормальний базис існує для кожного скінченного поля характеристики 2. Нормальний базис називається *гаусівським оптимальним нормальним базисом типу* 2, якщо число $p' = 2m+1$ – просте і для найменшого натурального числа k, такого що $2^k \equiv 1 \bmod (p')$, виконується одна з наступних умов:

а) $p' \equiv 1 \bmod 4$ і $k = 2m$;

б) $p' \equiv 3 \bmod 4$ і $k = m$.

Надалі гаусівський оптимальний нормальний базис типу 2 називається просто *оптимальним нормальним базисом.* Оптимальний нормальний базис існує не для всіх скінченних полів характеристики 2. Якщо такий базис існує, то він однозначно задається степенем m основного поля. Елементи оптимального нормального базису є коренями деякого незвідного многочлена $p(t)$, який називається нормальним многочленом скінченного поля. Цей многочлен будується наступним чином:

1.Приймають $q(t) = 1$, $p(t) = t + 1$.

2.Від 1 до $m-1$ обчислюють*:* $r(t) = q(t)$; $q(t) = p(t)$; $p(t) = tq(t) + r(t)$.

Слідом tr(x) елемента x скінченного поля називається елемент цього поля, рівний $tr(x) = \sum_{i=0}^{m-1} x^{2^i}$

Слід елемента завжди дорівнює 0 або 1. Слід нульового елемента основного поля завжди дорівнює 0. Слід одиничного елемента основного поля дорівнює 1 тоді і тільки тоді, коли степінь основного поля m – непарне число.

Напівслідом $htr(x)$ елемента x основного поля непарного степеня m називається елемент цього поля, рівний $htr(x) = \sum_{i=0}^{(m-1)/2} x^{4^i}$.

В.3 Виконання операцій в поліноміальному базисі

Елементи скінченного поля в поліноміальному базисі зображаються многочленами степеня не більше $m-1$ або, що еквівалентно, двійковими рядками довжини m, що складаються з коефіцієнтів таких многочленів. Елементи базису пов'язані примітивним многочленом, що визначає поле. Тому операції додавання і множення у скінченному полі у цьому випадку – це операції над многочленами степеня не більше $m-1$ зі зведенням результату у разі потреби за модулем примітивного многочлена.

Додавання двох елементів скінченного поля можна виконувати або як додавання відповідних многочленів, або як порозрядне додавання за модулем 2 відповідних до цих многочленів двійкових рядків. При додаванні зведення за модулем примітивного многочлена не потребне.

Множення двох елементів скінченного поля виконується як множення відповідних многочленів з наступним зведенням результату за модулем примітивного многочлена.

Піднесення до квадрата у полі характеристики 2 – лінійна операція, тобто $(x+y)^2 = x^2 + y^2$. Тому піднесення до квадрата у такому полі проста і дуже швидка операція.

Найпрацемісткіша операція в скінченних полях – обчислення оберненого елемента. Звичайно для цього використовується узагальнений алгоритм Евкліда обчислення найбільшого спільного дільника двох многочленів $f(t)$ і $c(t)$, тобто многочлена найбільшого степеня, що ділить обидва ці многочлени. Цей алгоритм виражає найбільший спільний дільник $d(t)$ як $d(t)=a(t)f(t)+b(t)c(t)$, де $a(t)$ і $b(t)$ – деякі многочлени, що обчислюються при виконанні узагальненого алгоритму Евкліда. Цей алгоритм діє наступним чином:

1.Приймають $a(t)=1$, $d(t)=f(t)$, $u(t)=0$, $v(t)=c(t)$.

2.Якщо $v(t)=0$, то приймають $b(t)=\dfrac{d(t)+f(t)a(t)}{c(t)}$ та закінчують виконання алгоритму.

3. За допомогою ділення з залишком обчислюють $d(t)=q(t)v(t)+r(t)$, далі обчислюють $w(t)=a(t)+u(t)q(t)$, $a(t)=u(t)$, $d(t)=v(t)$, $u(t)=w(t)$, $v(t)=r(t)$ та переходять до кроку 2.

Якщо як $f(t)$ взяти примітивний многочлен поля, а замість $c(t)$ – многочлен, що зображує елемент поля, то $d(t)$ є одиничний многочлен і наведене вище співвідношення за модулем примітивного многочлена перетворюється у співвідношення $b(t)c(t)=1 \bmod f(t)$, тобто многочлен $b(t)$ зображує елемент, обернений до $c(t)$.

При виконанні обчислень у скінченному полі часто доводиться зводити результат за модулем примітивного многочлена. Якщо як примітивний многочлен обрано примітивний тричлен або п’ятичлен, то зведення виконується набагато швидше у порівнянні зі звичайним зведенням за Барретом [9] або Монтгомері [10], не кажучи вже про просте ділення з залишком. Наприклад, якщо використовується примітивний тричлен $f(t)=t^m+t^k+1, 0<k<m$, то зведення многочлена $g(t)=g_{2m-2}t^{2m-2}+\ldots+g_1t+g_0$ степеня не вищого за $2m-2$ за модулем цього примітивного тричлена виконується так:

Для i від $2m-2$ до m обчислюємо $g_{i-m} \leftarrow g_{i-m}+g_i$ і $g_{i-m+k} \leftarrow g_{i-m+k}+g_i$.

Отриманий в результаті многочлен $g_{m-1}t^{m-1}+\ldots+g_1t+g_0$ – шуканий.

Подібний алгоритм існує для зведення за модулем примітивного п’ятичлена.

В.4 Виконання операцій в оптимальному нормальному базисі

В оптимальному нормальному базисі операції виконуються над зображеннями елементів поля у вигляді двійкових векторів, що відповідають розкладам цих елементів за елементами базису.

Додавання виконується так само, як у поліноміальному базисі, тобто шляхом порозрядного додавання зображень елементів поля за модулем 2.

Піднесення до квадрата в оптимальному нормальному базисі є просто циклічний зсув вправо на одну позицію зображення елемента поля.

Множення в оптимальному нормальному базисі виконується складніше. Для виконання множення спочатку треба обчислити мультиплікативну матрицю M, яка складається з рядків, які є розкладом в оптимальному нормальному базисі m добутків елементів базису вигляду $x \cdot x^{2^j}$, $j=0,\ldots,m-1$, тобто

$$M=\begin{Bmatrix} x\cdot x \\ \ldots \\ x\cdot x^{2^j} \\ \ldots \\ x\cdot x^{2^{m-1}} \end{Bmatrix}$$

Перший розряд добутку z двох елементів поля x і y обчислюється за формулою

$$z_{m-1} = xMy^T,$$

де x – вектор-рядок, а y^T – вектор-стовпчик.

Наступні розряди добутку обчислюються за цією самою формулою, тільки замість самих векторів x і y^T використовуються їх послідовні циклічні зсуви на один розряд вліво. Нагадаємо, що при використанні оптимального нормального базису крайній правий розряд зображення елемента поля відповідає елементу базису $x^{2^{m-1}}$. Складність множення визначається числом ненульових елементів у матриці M. В загальному випадку в цій матриці не менше $2m-1$ ненульових елементів. Якщо нормальний базис оптимальний, то ненульових елементів рівно $2m-1$, власне, з цієї причини такий базис і називається оптимальним. Повний опис умов існування оптимальних нормальних базисів надано в [11].

Практично замість мультиплікативної матриці обчислюються явні формули, які виражають один розряд добутку через розряди співмножників

Для обчислення оберненого елемента в оптимальному нормальному базисі використовується наступна формула: $x^{-1} = x^{2^m-2}, \quad x \neq 0$. Для обчислення правої частини цієї формули існує ефективний алгоритм [12]: нехай $m_r,\ldots,m_0$ – двійковий розклад цілого числа $m-1$. Тоді обчислення оберненого елемента виконується наступним чином:

1. $b \leftarrow x; k \leftarrow 1;$

2. Для i від $r-1$ до 0 обчислюють

2.1 $c \leftarrow b;$

2.2 Для j від 1 до k обчислюють

2.2.1 $c \leftarrow c^2;$

2.3 $b \leftarrow bc;$

2.4 $k \leftarrow 2k;$

2.5 Якщо $m_i = 1$, то $b \leftarrow b^2 x$ і $k \leftarrow k+1;$

3. $x^{-1} = b^2$

В.5 Многочлени над скінченними полями

Добуток всіх незвідних многочленів над полем $GF(2)$, степінь яких ділить ціле число k, дорівнює $t^{2^k} + t$. Тому многочлен $f(t)$ степеня *m* незвідний над полем $GF(2)$ тоді і тільки тоді, коли найбільший спільний дільник многочленів $t^{2^k} + t$ і $f(t)$ дорівнює 1 для всіх k таких, що $1 \le k \le \lfloor m/2 \rfloor$. Ця властивість дає ефективний алгоритм перевірки незвідності многочленів.

Нехай $p_1, \ldots, p_r$ – прості дільники числа $2^m - 1$. Незвідний многочлен над полем $GF(2)$ примітивний тоді і тільки тоді, коли

$t^{\frac{2^m-1}{p_i}} \neq 1 \bmod f(t)$ для всіх i, $1 \le i \le r$.

Ця властивість теж дає змогу легко побудувати ефективний алгоритм перевірки примітивності многочленів.

В алгоритмі з 6.11 обидва ці алгоритми використовуються сумісно. Розклади на прості множники чисел вигляду $2^m - 1$, необхідні для перевірки примітивності многочленів, наведено в таблицях [13].

Незвідний над полем $GF(2)$ многочлен $f(t)$ має m різних коренів у полі $GF(2^m)$. Знайти один із цих коренів можна наступним чином.

Нехай deg(·) позначає степінь многочлена, що міститься в дужках.

1. Приймають $g(t) = f(t)$.

2. Доки deg(*g*)>1, виконують наступні дії:

2.1 Обирають одночлен $d(t) = ut$ з випадковим коефіцієнтом $u \in GF(2^m)$;

2.2 Виконують $m-1$ раз обчислення $d(t) \leftarrow (d(t)^2 + ut) \bmod g(t)$.

2.3 Обчислюють найбільший спільний дільник $h(t)$ многочленів $g(t)$ і $d(t)$. Якщо deg(*h*)=0 або deg(*h*)=deg(*g*), то переходять до кроку 2.1. Якщо 2deg(*h*)>deg(*g*), то $g(t) \leftarrow g(t) / h(t)$, інакше приймають $g(t) = h(t)$. Переходять до кроку 2.1.

3. Маємо двочлен вигляду $g_1 t + g_0$. Тоді шуканий корінь дорівнює $g_0 g_1^{-1}$.

В.6 Заміна базису

Основне поле можна задавати поліноміальними базисами з різними примітивними многочленами або оптимальним нормальним базисом. Тому при реалізації цього стандарту може виникнути потреба переходити від одного базису до іншого.

Нехай скінченне поле задано базисом B_1, якому відповідає многочлен $p_1(t)$ (примітивний многочлен у разі поліноміального базису або нормальний многочлен у разі оптимального нормального базису) та базисом B_2, якому відповідає многочлен $p_2(t)$ (примітивний многочлен у разі поліноміального базису або нормальний многочлен у разі оптимального нормального базису). Для переходу від базису B_1 до базису B_2 обчислюють корінь u многочлена $p_1(t)$ в базисі B_2, а потім в базисі B_2 обчислюють елементи $u_k = u^k, 0 \le k \le m-1$, якщо базис B_1 поліноміальний, або елементи $u_k = u^{2^k}, 0 \le k \le m-1$, якщо базис B_1 оптимальний нормальний. З цих елементів будують матрицю U, що складається з їх розкладів у базисі B_2:

$$U = \begin{Bmatrix} u_0 \\ \dots \\ u_k \\ \dots \\ u_{m-1} \end{Bmatrix} = \begin{Bmatrix} u_{00} & \dots & u_{0m-1} \\ \dots & \dots & \dots \\ u_{m-1,0} & \dots & u_{m-1,m-1} \end{Bmatrix}$$

Ця матриця є матриця переходу від базису B_1 до базису B_2, а обернена матриця U^{-1} є матриця переходу від базису B_2 до базису B_1, тобто елемент поля в базисі B_1 (позначимо його x) та базисі B_2 (позначимо його y) пов'язані співвідношенням

$$y = xU,\ x = yU^{-1}.$$

В.7 Еліптичні криві над скінченними полями

Еліптична крива над скінченним полем $GF(2^m)$ є множина пар (x, y) елементів цього скінченного поля, що задовольняють афінне *рівняння еліптичної кривої* в нормальній формі Вейєрштрасса

$$y^2 + xy = x^3 + Ax^2 + B,$$

де $A, B \in GF(2^m),\ B \ne 0$,

разом із приєднаною *нескінченно віддаленою точкою* O. Пара (x, y) елементів основного поля називається афінними *координатами точки* еліптичної кривої. Нескінченно віддалена точка O не має афінних координат. Елементи (A, B) основного поля називаються *коефіцієнтами* рівняння еліптичної кривої. Координати точки P еліптичної кривої позначають (x_P, y_P). Число точок еліптичної кривої (враховуючи і нескінченно віддалену точку) називається *порядком* еліптичної кривої.

Поряд з афінним зображенням еліптичних кривих і точок на них відомі проективні зображення еліптичних кривих і точок на них декількох типів. Класичне проективне рівняння Вейєрштрасса має вигляд:

$$y^2z + xyz = x^3 + Ax^2z + Bz^3,$$

а точками проективної еліптичної кривої є трійки елементів основного поля $(x : y : z)$, що задовольняють це рівняння, причому хоча б одна з цих координат відмінна від нуля. Використання двокрапки у запису проективних координат позначає, що трійки координат, отримані одна з іншої множенням на ненульовий елемент основного поля, відповідають тій самій проективній точці еліптичної кривої (і також задовольняють проективне рівняння Вейєрштрасса). В проективному зображенні нескінченно віддалена точка має координати $(0:1:0)$. Для переходу від афінних координат до проективних використовуються співвідношення:

$(x, y) \to (x : y : 1);$

$O \to (0:1:0).$

Для переходу від проективних координат до афінних використовуються співвідношення:

Якщо $z = 0$, то $(x : y : z) \to O;$

Якщо $z \neq 0$, то $(x : y : z) \to (xz^{-1}, yz^{-1})$.

Перехід до проективних координат часто дає змогу підвищити ефективність обчислень у групі точок еліптичної кривої [14].

Точки еліптичної кривої утворюють скінченну абелеву групу відносно операції додавання точок. Правила виконання цієї операції наведено в наступному розділі. *Сума* точок P і Q еліптичної кривої позначається $P + Q$, при цьому $P + Q = Q + P$. Нейтральним (або нульовим) елементом цієї групи є нескінченно віддалена точка O: для будь-якої точки P еліптичної кривої виконується $P + O = O + P$. Точка $(-P)$, така, що $(-P) + P = P + (-P) = O$, називається точкою, *протилежною* для точки P, її координати виражаються через координати точки P наступним чином: $x_{-P} = x_P, y_{-P} = x_P + y_P$. Точка $2P = P + P$ називається по*двоєнням* точки P. Існує єдина точка порядку два, $P = (0, \sqrt{B})$. Сума k точок P, k – натуральне число, позначається kP, операція обчислення цієї суми називається множенням точки P на натуральне число k. За означенням $0P = O$, $(-k)P = k(-P)$, тому можна говорити про множення точки на довільне ціле число. Множення точки на ціле число – основна криптографічна операція, яка використовується у цьому стандарті. Еліптична крива з даним коефіцієнтом $B \neq 0$ ізоморфна у полі непарного степеня m або еліптичній кривій з коефіцієнтами $(0, B)$, або еліптичній кривій з коефіцієнтами $(1, B)$. Тому в стандарті прийнято, що коефіцієнт A дорівнює або 0, або 1

Нехай n – просте непарне число, що ділить порядок еліптичної кривої. Точка $P \neq O$ еліптичної кривої називається *базовою*, якщо її порядок дорівнює n, тобто $nP = O$ і $kP \neq O$, $0 < k < n$. Просте число n називається *порядком базової точки*. Порядок базової точки повинен задовольняти умову Менезеса-Окамото-Венстона [16,17], а саме, $2^{mk} \neq 1 \bmod n$ для $k = 1, \ldots, L_{MOV}$, де L_{MOV} – деяке граничне значення. Для скінченних полів, наведених у таблицях 1 і 2, достатньо прийняти L_{MOV}=32. Виконання цієї умови забезпечує високу криптографічну стійкість алгоритму обчислення й перевірки цифрового підпису, визначеного цим стандартом. Точки еліптичної кривої вигляду kP, $k = 0, \ldots, n-1$, утворюють циклічну підгрупу групи точок еліптичної кривої. Ця циклічна підгрупа є основною математичною структурою, в якій діють криптографічні алгоритми, встановлені в цьому стандарті.

Зображення точки P еліптичної кривої парою координат (x_P, y_P) є надмірним, оскільки координата y_P є один з двох розв'язків квадратного рівняння $y + x_P y = x_P^3 + A x_P^2 + B$. Якщо точка P має простий порядок, а степінь поля – непарне число, то наймолодший розряд координати x_P також надмірний, оскільки у цьому випадку $tr(A) = tr(x_P)$ [15] і наймолодший розряд x_P легко відновлюється за значенням сліду коефіцієнта A. Ці дві властивості дають змогу зображати точку еліптичної кривої у вигляді одного елемента основного поля. Таке зображення точок еліптичної кривої називається стиском точки.

В.8 Обчислення в групі точок еліптичної кривої

Нехай $P = (x_P, y_P)$, $P \neq O$ і $Q = (x_Q, y_Q)$, $Q \neq O$, $P \neq Q$ – дві точки еліптичної кривої в афінних координатах. Сума цих точок $R = P + Q$ обчислюється за такими правилами.

Якщо $Q = -P$, то $R = O$. Якщо $Q \neq -P$, то координати (x_R, y_R) точки R обчислюються за формулами:

$$x_R = \left(\frac{y_P + y_Q}{x_P + x_Q} \right)^2 + \frac{y_P + y_Q}{x_P + x_Q} + x_P + x_Q + A,$$

$$y_R = \left(\frac{y_P + y_Q}{x_P + y_Q} \right)(x_P + x_R) + x_R + y_P.$$

Якщо $x_P = 0$, то $2P = O$. Якщо $x_P \neq 0$, то координати (x_R, y_R) подвоєної точки $R = 2P$ обчислюються за формулами:

$$x_R = x_P^2 + \frac{B}{x_P^2},$$

$$y_R = x_P^2 + \left(x_P + \frac{y_P}{x_P} \right) x_R + x_R.$$

Для множення точки $P \neq O$ на велике ціле число можна використовувати способи, цілком аналогічні тим, що застосуються для піднесення цілого числа до степеня k. Наприклад, якщо $k = \sum_{i=0}^{t-1} k_i 2^i$ – двійкове зображення числа k, то точку $Q = kP$ можна обчислити наступним чином:

1.Приймають $Q \leftarrow O$.

2.Для i від t-1 до 0 обчислюють $Q \leftarrow 2Q$; якщо $k_i = 1$, то додатково обчислюють $Q \leftarrow Q + P$.

Як було відзначено вище, підвищити ефективність обчислень у групі точок еліптичної кривої можна за рахунок переходу до проективних координат. Це пов'язане з тим, що при додаванні й подвоєнні точок у проективних координатах не використовується операція обчислення оберненого елемента основного поля – найпрацемісткіша операція в скінченному полі.

В.9 Доведення правильності алгоритму перевірки цифрового підпису

Основне криптографічне перетворення при обчисленні цифрового підпису виконується над елементом h основного поля, який обчислюється за результатом обчислення функції гешування. Якщо отримане повідомлення ідентичне оригінальному, то при перевірці підпису буде обчислено точно той самий елемент основного поля. Якщо цифровий підпис прийнято без спотворень, то для перевірки цифрового підпису буде використана та сама пара цілих чисел (r, s), яка була отримана під час обчислення цифрового підпису. При перевірці цифрового підпису обчислюють точку еліптичної кривої $R = sP + rQ$, де P – базова точка еліптичної кривої, $Q = -dP$ – відкритий ключ цифрового підпису, обчислений за базовою точкою P з використанням особистого ключа цифрового підпису d. Крім того, $s=e+rd$, де e – одноразовий таємний параметр, який було використано для обчислення передпідпису (e, F_e). Тому

$$R = sP + rQ = (e + rd)P - rdP = eP + rdP - rdP = eP .$$

Таким чином, координата x_R точки $R = (x_R, y_R)$ дорівнює F_e, тому $y = hx_R = hF_e$ і після перетворення елемента y на ціле число $\tilde{r}$ отримаємо ціле число r, тобто $r = \tilde{r}$, що й доводить правильність алггоритму перевірки цифрового підпису.

Криптографічна стійкість цифрового підпису базується на дуже великій складності задач дискретного логарифмування $R = eP, Q = -dP$ в циклічній підгрупі групи точок еліптичної кривої, що використовується в цьому стандарті.

ДОДАТОК Г
(рекомендований)
РЕКОМЕНДОВАНІ ЕЛІПТИЧНІ КРИВІ

Для реалізації цього стандарту можна використовувати еліптичні криві, наведені в таблицях Г.1 і Г.2. В поліноміальному базисі зображення коефіцієнта *B* відповідає рекомендованому примітивному многочлену. Символ "/" означає, що написання коефіцієнта *B* еліптичної кривої або її порядку *n* розділено на два рядки.

Таблиця Г.1 – Рекомендовані еліптичні криві в поліноміальному базисі

№ ч/ч	m	Еліптична крива
1	163	A=1 B=5FF6108462A2DC8210AB403925E638A19C1455D21 n=400000000000000000002BEC12BE2262D39BCF14D
2	167	A=1 *B*=6EE3CEEB230811759F20518A0930F1A4315A827DAC *n*=3FFFFFFFFFFFFFFFFFFFFB12EBCC7D7F29FF7701F
3	173	A=0 B=108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9 n=800000000000000000000189B4E67606E3825BB2831
4	179	A=1 B=4A6E0856526436F2F88DD07A341E32D04184572BEB710 n=3FFFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF
5	191	A=1 B=7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03 n=400000000000000000000000069A779CAC1DABC6788F7474F
6	233	A=1 B=06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA/ 936ECE454D2C n=1000000000000000000000000000013E974E72F8A6922031D2/ 603CFE0D7
7	257	A=0 B=1CEF494720115657E18F938D7A7942394FF9425C1458C5786/ 1F9EEA6ADBE3BE10 n= 800000000000000000000000000000006759213AF182E987D3/ E17714907D470D
8	307	A=1 B=393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E24/ 1050DF18B6090BDC90186904968BB n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC079C2F38/ 25DA70D390FBBA588D4604022B7B7
9	367	A=1 *B*=43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64/ B0C2AFE42CADAB8F93D92394C79A79755437B56995136 n=4000000000000000000000000000000000000000000009C300/ B75A3FA824F22428FD28CE8812245EF44049B2D49
10	431	A=1 B=03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D 28AA/

		EAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3 n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF/ BA3175458009A8C0A724F02F81AA8A1FCBAF80D90C7A95110504CF

Таблиця Г.2 - Рекомендовані еліптичні криві в оптимальному нормальному базисі

№ ч/ч	m	Еліптична крива
1	173	A=0 B=043D7E139319F43BA00944915740E1E6651B06E278C7 n=800000000000000000000189B4E67606E3825BB2831
2	179	A=1 B=0B151F20BCB9AC860B2F2CCE4F5E27EC1840C9E9D30BB n=3FFFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF
3	191	A=1 B=09C38E4E94EB67753A07EABA227B97EDD72ACE09D0F18F7C n= 400000000000000000000000069A779CAC1DABC6788F7474F
4	233	A=1 B=080F920952A702C75B704A424C018EEA55AA44664F3A003E0962D4F9A8E N= 1000000000000000000000000000013E974E72F8A6922031D2603CFE0D7
5	431	A=1 B=19794FD03E5CFCBC1B17A03BF8ED0D946F57FE2C1AE97E4A669FDBD7B/ DA20380053791356B5D6941BC3235EC1F8FCA04085260CA9B77 n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF/ BA3175458009A8C0A724F02F81AA8A1FCBAF80D90C7A95110504CF

ДОДАТОК Д
(довідковий)
БІБЛІОГРАФІЯ

1. Лиддл Р., Нидеррайтер Г. Конечные поля. Т.1 и 2. -М., Мир, 1988.-с.818.
2. Koblitz N. Elliptic Curve Cryptosystems// Mathematics of Computation. – 48. – 1987. – p. 203 – 209.
3. Miller V.S. Use of Elliptic Curves in Cryptography// Advances in Cryptology – Crypto'85. – LNCS 218. – 1986. – p. 417 – 426.
4. Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer, 1986. – p. 400.
5. Silverman J. Advanced Topics in the Arithmetic of Elliptic Curves. –New York: Springer, 1994. – p. 525.
6. Menezes A. Elliptic Curve Public Key Cryptosystems. – Boston: Kluwer Academic Publishers, 1993. –p. 126.
7. Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. – Cambridge University Press, 1999. – p.204.
8. Кочубинский А.И. Эллиптические кривые в криптографии. // Безопасность информации. – 2, – 2000. с.18-31.
9. Barrett P. Implementing the Rivest, Shamir and Addleman Public Key Encryption Algorithm on a Standard Digital Signal Processor.// Advances in Cryptology – Crypto'86 (LNCS 263), – 1986. –p.311-323.
10. Montgomery P. Modular Multiplication without Trial Division.// Mathematics of Computation. – 44, – 1985. –p.519-521.
11. Mullin R., Onyszczuk I., Vanstone S.A., Wilson R. Optimal Normal Bases in $GF\left(p^n\right)$.// Discrete Applied Math. – 22, – 1988/1989. p – 149-161.
12. Itoh T., Tsijii S. A Fast Algorithm for Computing Multiplicative Inverses in $GF\left(2^m\right)$ Using Normal Bases. // Info. and Comput. – 78(3), – 1988. – p.171-177.
13. Brillhart J., Lehmer D.H., Selfridge J,L., Tuckerman B., Wagstaff S.S., Jr. Factorizations of $b^n \pm 1$, b=2,3,5,6,7,10,11,12 up to high powers. // Contemporary mathematics, v.22. AMS, Providence, Rhode Island.
14. Cohen H., Miyaji A., Ono T. Efficient Elliptic Curves Exponentiation Using Mixed Coordinates.// Advances in Cryptology –Asiacrypt'98 (LNCS 1514), –1998. –51-65.
15. Seroussi G. Compact Representation of Elliptic Curve Points over $GF\left(2^m\right)$. // Hewlitt-Packard Laboratories Technical Report No HPL-98-135. – 1998.
16. Menezes A.J., Okamoto T., Vanstone S.A. Reducing Elliptic Curve Logarithms to a Finite Field.// IEEE Trans. Info. Theory. – 39, –1993. –p.1639-1646.
17. Balasubramanian R., Koblitz N. The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm// J. of Cryptology, – №2. – 11. – 1998. – p.141 – 145.
18. ГОСТ Р34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи.
19. IEEE Std 1363-2000 Standard Specification for Public-Key Cryptography.
20. Zemor. Cours de cryptographie Vuibert, 2000, - p. 212.

УКНД 35.040

Ключові слова: кодування інформації, захист інформації, криптографія, автентичність, неспростовність, цифровий підпис, особистий ключ, відкритий ключ, еліптичні криві