УДК 004.91

ПОЛТОРАК В.П.,
ГОЛКОВ В.Б.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СИСТЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ТА ОСОБЛИВОСТІ ЇХ РЕАЛІЗАЦІЇ НА ЕЛІПТИЧНИХ КРИВИХ

Робота присвячена огляду та аналізу алгоритмів формування електронного цифрового підпису. Порівнюються відомі алгоритми створення електронного цифрового підпису, розглядаються питання реалізації алгоритму електронного цифрового підпису на еліптичних кривих та пропонується схема його програмної реалізації.

The paper is devoted to the review and analysis of algorithms for creation electronic digital signature. Known electronic digital signature algorithms are compared, examined the questions of implementation of the elliptic curve digital signature algorithm, proposed scheme of its software implementation.

1. Вступ

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, комерційні і некомерційні організації, а також громадяни в своїх офіційних і особистих стосунках.

Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є Електронний цифровий підпис (ЕЦП), який забезпечує автентичність повідомлення та неспростовність застосування особистого ключа (автентифікація власника цифрового підпису)[1]. За допомогою спеціального програмного забезпечення ЕЦП підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою.

У даній роботі розглядаються методи створення ЕЦП та питання їх реалізації. ЕЦП являє собою реквізит електронного документу, що дозволяє встановити відсутність спотворення інформації в електронному документі з моменту формування ЕЦП і перевірити належність підпису власнику сертифіката ключа ЕЦП.

Використання ЕЦП дозволяє:

- замінити традиційні печатку та підпис при безпаперовому документообігу;
- удосконалити і здешевити процедуру підготовки, доставки, обліку і зберігання документів, гарантувати достовірність документації;
- значно скоротити час руху документів, прискорити і полегшити процес візування одного документу декількома особами;
- побудувати корпоративну систему обміну електронними документами;
- забезпечити цілісність – гарантію того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін.

Цифровий підпис провадить наступні функції [2]:

- автентифікація: для отримувача повідомлення повинна бути можливість переконатися в його достовірності;
- неможливість відмови від відправлення: відправник не повинен мати можливості заперечити відправлення та підпис повідомлення протягом деякого часу після відправлення;
- цілісність: отримувач повідомлення повинен мати можливість перевірити той факт, що повідомлення не було змінене при передачі.

Цифровий підпис повинен гарантувати наступні ознаки:

- немає можливості підробки підпису;
- підпис може бути перевіреним, засвідченим;
- після того, як повідомлення підписане, відправник не зможе відмовитися від факту його передачі.

2. Актуальність проблеми

На сьогоднішній день ЕЦП широко використовується юридичними та фізичними особами, активно впроваджується в державних установах і органах державної влади. У системах документообігу використовуються різні алгоритми

ЕЦП, і незважаючи на те, що загалом всі алгоритми виконують свої функції, між ними існує значна різниця, у кожного алгоритму є свої переваги та недоліки, які потребують дослідження. Таким чином, актуальність проблеми обумовлюється потребою вибору алгоритму ЕЦП, наявність власної його реалізації дозволить розширити можливості дослідження та аналізу якостей алгоритму, а також зіштовхне нас з проблемами практичного характеру.

3. Огляд існуючих рішень

Симетрична криптографія має, здавалося б, дуже просту і зрозумілу схему ключів – відправник і одержувач знають один загальний секрет, і третім особам він недоступний. Але ця на перший погляд зручна схема приховує в собі підводні камені при значному збільшенні числа абонентів, які бажають шифрувати взаємну переписку. Адже якщо користувач хоче конфіденційно вести справи з N партнерами, йому необхідно мати N секретних ключів, а загальна кількість ключів в системі зростає від кількості абонентів за формулою N*(N - 1)/2.

Крім того, з'являються питання довіреної доставки ключів абонентам і ситуації, коли одержувач, дешифрувавши повідомлення, може внести до нього зміни, а потім посилатися на документ, нібито вже отриманий у такому вигляді.

Асиметрична криптографія вирішує це питання кардинально інакше – по-перше кількість ключів скорочується до 2*N. Кожен абонент бере участь у спілкуванні в єдиному інформаційному полі, володіє двома ключами – відкритим (відомим всім іншим абонентам) і закритим (відомим тільки йому і зберігається ним у секреті). Відкритий ключ використовується для відправки повідомлень: з його допомогою на основі спеціального алгоритму будь-який бажаючий може зробити асиметричне шифрування – необоротне, без знання закритого ключа, перетворення документу. А ось дешифрувати повідомлення зможе лише власник закритого ключа, тобто законний одержувач.

Схеми ключів симетричною і асиметричною криптографії для порівняння наведені на рис. 1 та 2.

Ця робота зосереджена на дослідженні асиметричних схем цифрового підпису з доповненням (appendix) [2]. «Доповнення» означає, що використовується криптографічна хеш-функція для створення дайджесту повідомлення, і перетворення підпису повідомлення відбувається над дайджестом повідомлення, а не над власне повідомленням.

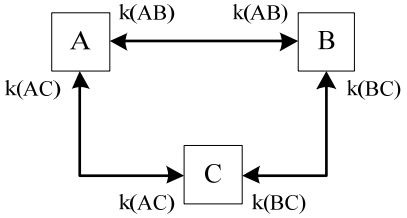

Рис. 1. Ключі в симетричній криптографії

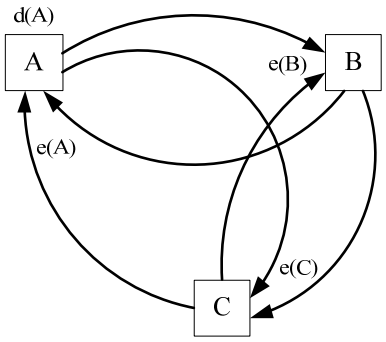

Рис. 2. Ключі в асиметричній криптографії

Сучасні схеми цифрового підпису можуть бути класифіковані таким чином відповідно до складної математичної проблеми, що лежить в їх основі, та забезпечує їх безпеку [3]:

1) Схеми факторизації цілих чисел (ФЦ), безпека яких залежить від складності розв'язку проблеми розкладу на множники (факторизації) цілих чисел. Прикладами цих схем є схеми підпису RSA та Рабіна.

2) Схеми дискретного логарифму (ДЛ), безпека яких залежить від складності розв'язку проблеми знаходження (звичайного) дискретного логарифму у скінченному полі. Прикладами є схеми підпису Ель-Гамаля, Шнорра, DSA.

3) Схеми на еліптичних кривих (ЕК), безпека яких залежить від складності розв'язку проблеми знаходження дискретного логарифму на ЕК. Прикладами є схеми підпису EC-KDSA, ECSS, ECDSA.

Схема цифрового підпису RSA. Для формування електронного підпису відправник виконує над контрольною сумою документу h ті ж самі дії, що і при шифруванні, але використовує не відкритий ключ одержувача, а свій власний закритий ключ, тобто $sign_i = (h_i^d \bmod n)$. Відкритий і закритий ключі просто міняються місцями. На приймальній стороні

одержувач зводить підпис у степінь відкритого ключа e відправника і отримує ($sign_i^e$ mod n) = (h_i^{de} mod n) = h_i (згідно з тими ж формулами, що і в асиметричному шифруванні RSA).

Якщо після зведення в степінь значення співпадає з обчисленою незалежно на приймальній стороні контрольною сумою документу, то перевірка вважається виконаною, а документ - справжнім. Ніхто, крім відправника, не знаючи d, не може обчислити такий підпис $sign_i$, щоб зведення її до рівня відкритого ключа e дало необхідну контрольну суму - це те ж саме важковирішуване завдання, що і в асиметричному шифруванні RSA. Отже, забезпечити документ таким підписом $sign_i$ міг тільки справжній власник закритого ключа. Схема ЕЦП наведена на рис. 3.

Схема цифрового підпису DSA. Згідно з FIPS Pub 186–2 (Federal Information Processing Standards (FIPS), 2000), DSA використовує наступні параметри:

1) p – простий модуль, де $2^{L-1} < p < 2^L$ для L=1024;

2) q – простий дільник p - 1, де $2^{159} < q < 2^{160}$;

3) $g = h^{(p-1)/q} \bmod p$, де h будь-яке ціле число в межах $1 < h < p-1$ таке що $h^{(p-1)/q} \bmod p > 1$ (g має порядок q mod p);

4) x = a випадково або псевдо випадково згенероване ціле число в межах $0 < x < q$;

5) $y = g^x \bmod p$;

6) k = a випадково або псевдо випадково згенероване ціле число в межах $0 < k < q$;

Цілі числа p, q, та g можуть бути відкриті та загальновідомі групі користувачів. Закритий та відкритий ключі користувача - це x і y, відповідно. Параметри x та k використовуються лише для генерації підпису, та повинні триматися в таємниці. Параметр k повинен змінюватися для кожного підпису.

Підписом для повідомлення m буде пара чисел r та s обчислених згідно з рівняннями: $r=(g^k \bmod p) \bmod q$, та $s=(k^{-1}(\mathrm{SHA}-1(m)+x\,r)) \bmod q$.

Вище згадане k^{-1} є мультиплікативною інверсією k, mod q, тобто, $(k^{-1} * k) \bmod q = 1$ та $0 < k^{-1} < q$. Значенням SHA−1(m) є 160-бітовий рядок, що є виходом алгоритму Secure Hash Algorithm, визначеного у стандарті FIPS 180-1, та повинен бути перетворений у ціле число. Підпис разом з повідомленням передається отримувачу.

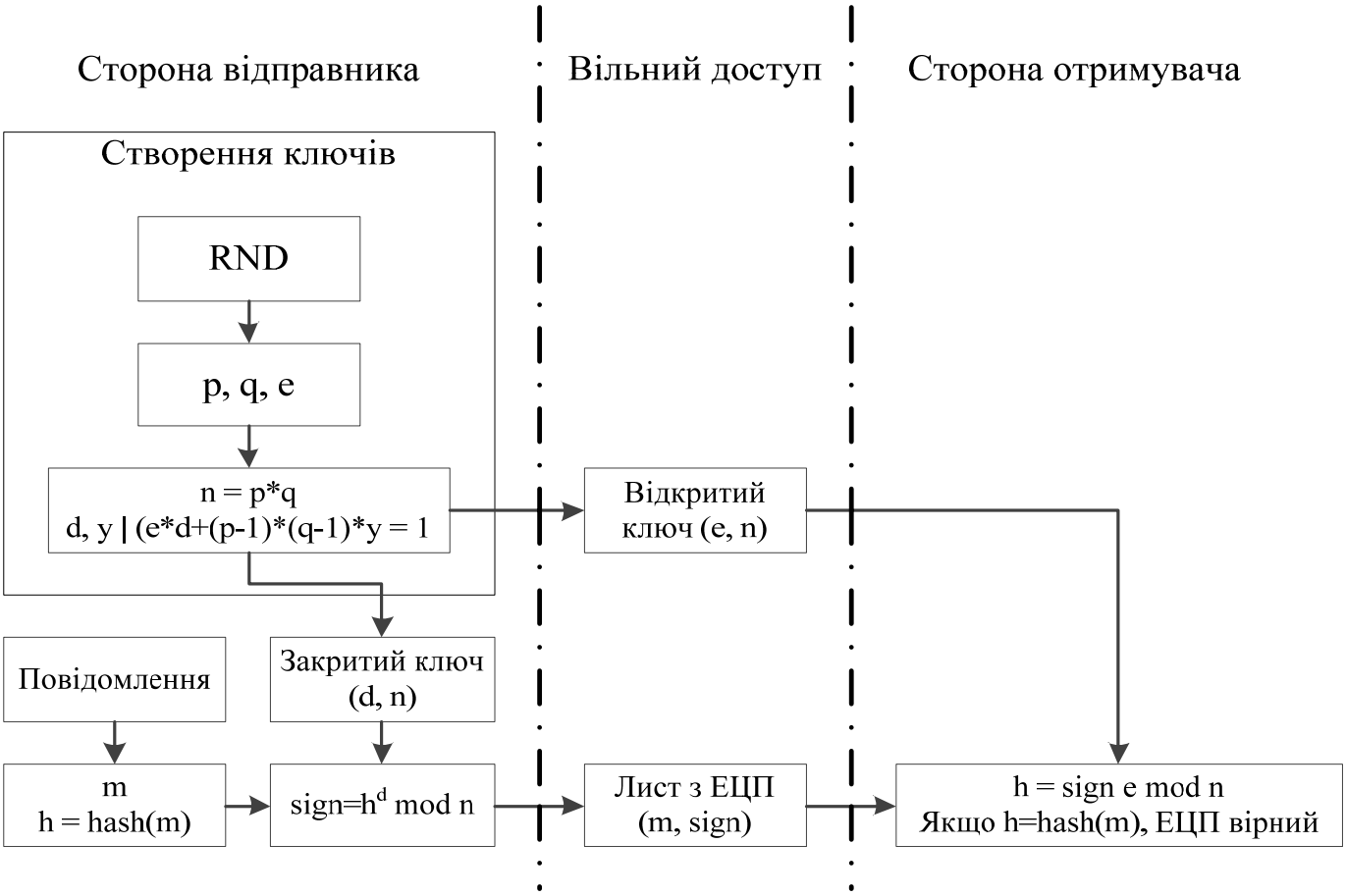

Рис. 3. Схема ЕЦП RSA

До процедури верифікації підпису необхідно отримати доступ до *p, q* та *g*. Як тільки відправник підписав повідомлення, він відправляє повідомлення, *m,* разом з цифровим підписом *r* та *s*.

Нехай *m′, r′,* та *s'* – це отримані версії *m, r,* та *s,* відповідно, та нехай *y* буде відкритим ключем відправника. Щоб перевірити підпис відправника, отримувач спершу перевіряє чи лежать в заданих межах $0 < r' < q$ та $0 < s' < q$.

Якщо ця умова порушена, то підпис відкидається. Якщо ці дві умови виконуються, тоді перевірник обчислює:

$$w = (s')^{-1} \bmod q$$

$$u_1 = ((SHA-1(m')w) \bmod q$$

$$u_2 = ((r')w) \bmod q$$

$$v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$$

Якщо *v=r′,* тоді підпис є вірним та перевірник може бути певним, що це повідомлення дійсно було відправлене особою, що має закритий ключ, *x,* що відповідає відкритому ключу *y*.

Якщо *v* не дорівнює *r′,* тоді повідомлення могло бути змінене, або невірно підписане Алісою, або повідомлення могло бути підписане зловмисником, та, таким чином, повідомлення повинне бути визнане недійсним [2].

Схема цифрового підпису ECDSA. ECDSA є одним з варіантів схеми підпису Ель-Гамаля. ECDSA з'явився як модифікація алгоритму DSA, з метою використання еліптичних кривих в якості основи обчислень. Згодом алгоритм знайшов визнання і на цей час використовується у декількох стандартах [3].

Розглянемо базову схему алгоритму:

1) Загальновідомі параметри: в алгоритмі можливе використання скінченних полів двох видів: поля характеристики два або великого простого поля. Надалі розглянемо в якості базового велике просте поле. Відкриті параметри складаються з поля порядку *p*, еліптичної кривої визначеної двома елементами поля *a* та *b*, простого числа *n* більшого ніж 2^{160} , та елемента *G* порядку *n*, що належить еліптичній кривій. Рівняння еліптичної кривої має вигляд $y^2 = x^3 + ax + b$. Відкриті параметри є об'єктом для багатьох критеріїв безпеки.

2) Підготовка: обрати випадкове ціле число *d* в межах [1, *n* - 1], обчислити $Q = dG$. На виході отримаємо $(K_p, K_s) = (Q, d)$.

3) Генерація підпису:обрати випадкове ціле число *k* в межах [1, *n* - 1] та обчислити:

$$(x_1, y_1) = kG;$$

$$r = \bar{x}_1 \bmod n;$$

$$s = \frac{H(M) + ar}{k} \bmod n.$$

Тут $\bar{x}_1$ є певним чином перетворений в ціле число елемент скінченного поля x_1 . Якщо $r = 0$ або $s = 0$, знову переходимо на крок вибору *k*. Виходом процедури генерації підпису буде пара $\sigma = (r, s)$

4) Верифікація підпису: перевірити, що $Q \neq O$, $Q \in C$, та $nQ = O$. Перевірити, що *r* та *s* лежать в межах [1, *n* - 1] і $r = x_1 \bmod n$ для $(x_1, y_1) = u_1 G + u_2 Q$, $u_1 = \frac{H(M)}{s} \bmod n$, та $u_2 = \frac{r}{s} \bmod n$.

Складність алгоритму ECDSA полягає в необхідності роботи з об'єктами різних типів: точки еліптичної кривої, елементи поля, цілі числа, та рядки бітів. В стандартах, що використовують даний алгоритм, наведений докладний опис про способи представлення цих об'єктів та способи маніпуляції ними.

4. Порівняльний аналіз криптостійкості алгоритмів підпису

З трьох проблем, що використовуються в асиметричних схемах підпису, проблема факторизації цілих чисел та дискретного логарифму можуть бути вирішені алгоритмами, які виконуються за субекспоненційний час. Це означає, що проблема визнана досить важкою, але не настільки важкою як ті проблеми, що вирішуються алгоритмами лише за повністю експоненційний час. З іншого боку, найкращий алгоритм загального спрямування для проблеми дискретного логарифму в групі точок еліптичної кривої (ПДЛЕК) виконується за повністю експоненційний час. Це означає, що ПДЛЕК наразі визнана більш складною ніж проблема факторизації цілих чисел або проблема дискретного логарифму (ПДЛ).

Маючи на увазі цю властивість криптосистем на еліптичних кривих, висока безпека при відносно невеликому розмірі ключа, дослідимо властивості систем на еліптичних кривих порівняно з іншими криптосистемами ЕЦП.

Проблема факторизації цілих чисел (ПФЧ) полягає в наступному: маючи складене число *n*,

що є добутком двох великих простих цілих чисел p та q, знайти p та q. В той час як знаходження двох великих простих чисел є досить простим завданням, проблема розкладання добутку двох таких чисел на множники визнана обчислювально складною, якщо прості числа обрані належним чином. Схема ЕЦП RSA базується на цій проблемі.

Існує два основних типи алгоритмів факторизації [4]: загального спрямування та спеціалізованого спрямування. Алгоритми факторизації спеціалізованого спрямування намагаються використати спеціальні ознаки числа n, яке розкладається. На відміну від них, час виконання алгоритмів факторизації загального спрямування залежить лише від розміру числа n.

Одним з найбільш потужних алгоритмів факторизації спеціалізованого спрямування є метод факторизації з використанням еліптичних кривих (ECM), що був винайдений в 1985 році Хендріком Ленстрою. Час виконання цього алгоритму залежить від розміру простих множників числа n, тому в першу чергу алгоритм намагається знайти малі множники. Найбільшим простим множником знайденим на цей час за допомогою ECM є множник з 54 цифр (180 біт) числа з 127 цифр (422 біта) [4].

До розробки криптосистеми RSA, кращим алгоритмом факторизації загального спрямування був алгоритм неперервних дробів, який міг розкладати на множники числа до 40 десяткових цифр (133 біта). Цей алгоритм заснований на ідеї використання базового множника простого числа та генерації відповідної множини лінійних рівнянь, вирішення яких обов'язково приведе до розкладання на множники. Ця ідея лежить в основі і кращих алгоритмів, що використовуються на даний момент: квадратичне решето (QS) та загальне решето числового поля (NFS). Обидва алгоритми легко можуть виконувати факторизацію паралельно у розподілених мережах робочих станцій.

Квадратичне решето було використане, щоб розкласти на множники число з 129 десяткових цифр (429 біт), що було числом-викликом RSA поставленим в 1977 році.

Загальне решето числового поля, розроблене в 1989 році, найкраще працює на числах спеціальної форми (512+1). Згодом воно було розширене до алгоритму факторизації загального спрямування. Нещодавні експерименти довели, що NFS є дійсно потужним алгоритмом для розкладання на множники цілих чисел, що мають щонайменше 130 цифр (432 біта) [4].

Проблема дискретного логарифму в простому полі. Якщо p є простим числом, тоді Z_p визначає множину чисел {0, 1, 2, …, p-1}, де додавання та множення виконуються по модулю p.

Проблема дискретного логарифмування в скінченному полі (ПДЛ) полягає в наступному: маючи просте число p, генератор α Z_p, та ненульовий елемент $\beta \in Z_p$, знайти унікальне ціле число $l, 0 \le l \le p-2$, таке що $\beta \equiv \alpha^l \pmod p$. Ціле число l називається дискретним логарифмом β за базою α [4].

Базуючись на складності цієї проблеми, Діффі та Хеллман запропонували відому схему обміну ключами в 1976 році. З того часу багато інших криптографічних протоколів, чия стійкість залежить від ПДЛ, були запропоновані, включаючи DSA, схему Ель-Гамаля та схему Шнорра. Через інтерес до цих застосувань ПДЛ інтенсивно вивчалась математиками останні 20 років.

Як і з проблемою факторизації цілих чисел, існують два типи алгоритмів для вирішення проблеми дискретного логарифму. Алгоритми факторизації спеціалізованого спрямування намагаються використати спеціальні ознаки числа p, яке розкладається. На відміну від них, час виконання алгоритмів факторизації загального спрямування залежить лише від розміру числа p.

Найшвидші відомі алгоритми загального спрямування для вирішення ПДЛ засновані на методі, що називається індексне або диференційне обчислення. В цьому методі, створюється база даних з малих простих чисел та відповідних їм логарифмів, згідно з якою можуть бути отримані логарифми випадкових елементів поля. Це нагадує методи з базовим множником для проблеми факторизації. Тому якщо відбудеться прогрес в алгоритмі вирішення однієї з проблем, скоро після цього схожий покращений алгоритм буде знайдено і для іншої проблеми.

Найкращим відомим алгоритмом для вирішення ПДЛ на даний момент є загальне решето числового поля. Він має такий ж асимптотичний час виконання, що й відповідний алгоритм для факторизації цілих чисел. З цього можна

зробити висновок, що проблема знаходження логарифмів у випадку простого числа p розміром k біт має приблизно таку ж складність, що й розкладання складеного числа n розміром k біт. В 1998 році було оголошено розв'язок Виклику Діффі-Хеллмана, який включав вирішення ПДЛ по модулю простого числа з 129 цифр. Використане просте число мало спеціальну форму, тому був використаний алгоритм загального решета числового поля, який був дуже ефективним для цього виклику. Ці результати є доказами довгострокової безпеки, в криптосистемах, що використовують ПДЛ, слід використовувати модуль p розміром 1024 біта або більше [4].

Проблема дискретного логарифму у групі точок еліптичної кривої, визначеної над простим полем. Якщо p є простим ступенем, то F_p визначає скінченне поле, що містить p елементів. В застосуваннях p зазвичай є ступенем 2 (2^m) або непарним простим числом (p).

Проблема дискретного логарифму в групі точок еліптичної кривої (ПДЛЕК) полягає в наступному: маючи еліптичну криву E визначену над полем F_p, точку $G \in E(F_p)$ порядку n, і точку $Q \in E(F_p)$, необхідно визначити ціле число $l, 0 \le l \le n-1$, таке що $Q = lG$, за умови, що таке ціле число існує.

Базуючись на складності цієї проблеми, було запропоновано використання групи точок еліптичної кривої визначеної над скінченним полем для реалізації різних криптосистем. Один з таких протоколів є аналог DSA на еліптичних кривих, алгоритм ECDSA. Таким чином, ПДЛЕК може розглядатися як схожа на проблему ПДЛ, але в іншому алгебраічному середовищі.

З 1985 року ПДЛЕК привернула значну увагу провідних математиків з усього світу. Алгоритм Похліга та Хеллмана [3,5] скоротив визначення l до визначення кожного з множників n по модулю l. Тобто, щоб досягнути максимального рівня безпеки, необхідно щоб n було простим числом. Кращим алгоритмом загального спрямування для вирішення ПДЛЕК на даний момент є метод Полларда, який з прискоренням запропонованим Галлантом, Ламбертом та Венстоном, має близько $\sqrt{\pi n}/2$ кроків, де під кроком маємо на увазі операцію додавання в групі точок еліптичної кривої.

Найважливішим є те, що для ПДЛЕК не відомо жодного алгоритму типу індексного обчислення на відміну від ПДЛ. Тому вирішення ПДЛЕК вважається складнішим ніж проблеми факторизації цілих чисел або ПДЛ, оскільки невідомо алгоритму загального спрямування з субекспоненційним часом виконання.

В 1991 році Менезес, Окамото та Венстон (MOV) [4] показали, як ПДЛЕК може бути скорочено до ПДЛ в розширенні полів F_p, де можна використати методи індексного обчислення. Тим не менш, цей алгоритм скорочення MOV ефективний тільки для дуже особливого класу кривих, відомих як суперсингулярні криві. Крім того, існує простий тест, за допомогою якого можна перевірити, що окрема еліптична крива не є вразливою до цієї атаки. Суперсингулярні криві є спеціально забороненими в усіх стандартах з використанням систем на ЕК, таких як IEEE P1363, ANSI X9.62, та ANSI X9.63.

Іншим так званим слабким класом еліптичних кривих є так звані аномальні криві – це криві E визначені над полем F_p, котре має кількість точок, що дорівнює точно p. Атака на ці криві була винайдена незалежно Семаєвим, Смартом та Сато і Аракі, та узагальнена Рюком. Як і у випадку з суперсингулярними кривими, існує простий тест, за допомогою якого можна перевірити, що окрема еліптична крива не є вразливою до цієї атаки.

Дослідження ПДЛЕК та пов'язаних з нею проблем та пошук нових рішень продовжується і на цей час. Необхідно відзначити, що в вище описаних програмних та апаратних атаках, обчислення єдиного дискретного логарифму в групі точок еліптичної кривої має ефект розкриття одного закритого ключа користувача. Ті самі зусилля необхідні для визначення другого закритого ключа користувача.

На графіку на рис. 4 порівнюється час, потрібний для злому ECDSA з часом необхідним для злому RSA або DSA для різних розмірів ключа з використанням найкращих відомих алгоритмів [5]. Значення обчислені в MIPS роках. MIPS рік представляє час обчислення, що дорівнює 1 року на машині спроможній виконувати 1 мільйон інструкцій в секунду. Для порівняльного тесту, загальноприйнятим є те, що 10^{12} MIPS років представляє значну безпеку на даний момент, оскільки таке значення потребує, щоб більшість обчислювальної потужності на планеті працювала значний проміжок часу. Щоб досягти такого рівня безпеки RSA та DSA необхідно використовувати ключ розмі-

ром 1024 біт, в той час як для алгоритму ECDSA достатньо ключа розміром 160 біт.

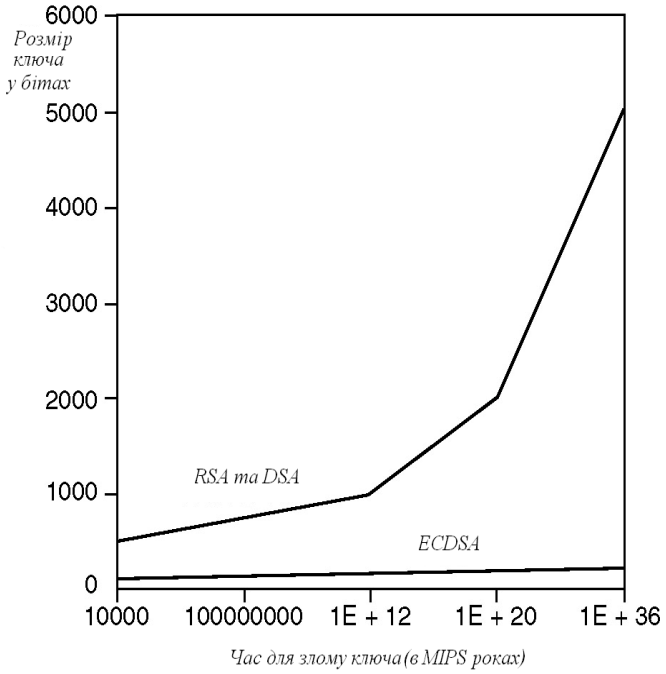

Рис. 4. Порівняння рівнів безпеки криптосистем ЕЦП

Зауважимо, що різниця між системами зростає по мірі збільшення розміру ключа. Наприклад, помітимо, як значення обсягу обчислень зростає для ECDSA з ключем розміром 300 біт порівняно з RSA та DSA з ключами розміром 2048 біт.

Порівняння трьох складних математичних проблем, на яких базуються відомі асиметричні криптосистеми підпису виявило той факт, що жодна з них не є доказово надійною. Роки інтенсивних досліджень призвели до загальноприйнятого переконання, що ПДЛЕК значно складніша ніж проблема факторизації цілих чисел та ПДЛ. Загальним висновком є те, що ПДЛЕК потребує повністю експоненційного часу для вирішення.

Розглянувши основні схеми постановки електронного цифрового підпису та аналізу їх переваг та недоліків, отримані результати можна звести до наступної табл. 1 для значення 10^{11} MIPS років необхідних для злому закритого ключа.

5. Принципи та особливості реалізації системи ЕЦП

Була розроблена система ЕЦП, що реалізує алгоритм ECDSA, так як даний алгоритм має ряд переваг, описаних вище, у порівнянні з іншими алгоритмами ЕЦП.

До розроблюваної системи ставились наступні вимоги:

- Можливість встановити порядок p еліптичної кривої у діапазоні [3; 2^{521}], що надає гнучкі засоби для вивчення та дослідження алгоритму;
- Можливість використання так званих аномальних та суперсингулярних кривих для дослідження їх уразливості;
- Побудова графіку еліптичної кривої невеликого порядку, наочне виконання операцій над точками побудованої еліптичної кривої;
- Поетапне відображення процедур постановки та верифікації ЕЦП;
- Можливість підстановки зміненого документу та його підпису на етапі верифікації підпису у цілях дослідження.

На рис. 5 представлена блок-схема реалізованого алгоритму постановки ЕЦП на основі алгоритму ECDSA.

Табл. 1. Порівняння сучасних алгоритмів цифрового підпису

Ознака порівняння	Алгоритм ЕЦП		
	RSA	DSA	ECDSA
Проблема що лежить в основі алгоритму	ПФЧ	ПДЛ	ПДЛЕК
Розмір системних параметрів в бітах	1024	2208	481
Розмір отриманого підпису в бітах	1024	320	320
Розмір відкритого ключа в бітах	1088	1024	161
Розмір закритого ключа в бітах	2048	160	160

У блоках 3 і 6 блок-схеми, представленої на рис. 5, виконується операція множення точки еліптичної кривої на число. Дана операція потребує значної кількості обчислень, так як в математичному апараті еліптичних кривих над скінченим полем не існує операції множення точки на число, більше 2, тому необхідне багаторазове виконання операції додавання точок.

При такому підході у разі виконання операції множення точки P на число k, необхідна одна операція знаходження точки 2P та k - 2 операцій додавання, які потребують великої кількості часу при значеннях числа k порядку 2^{160} і більше.

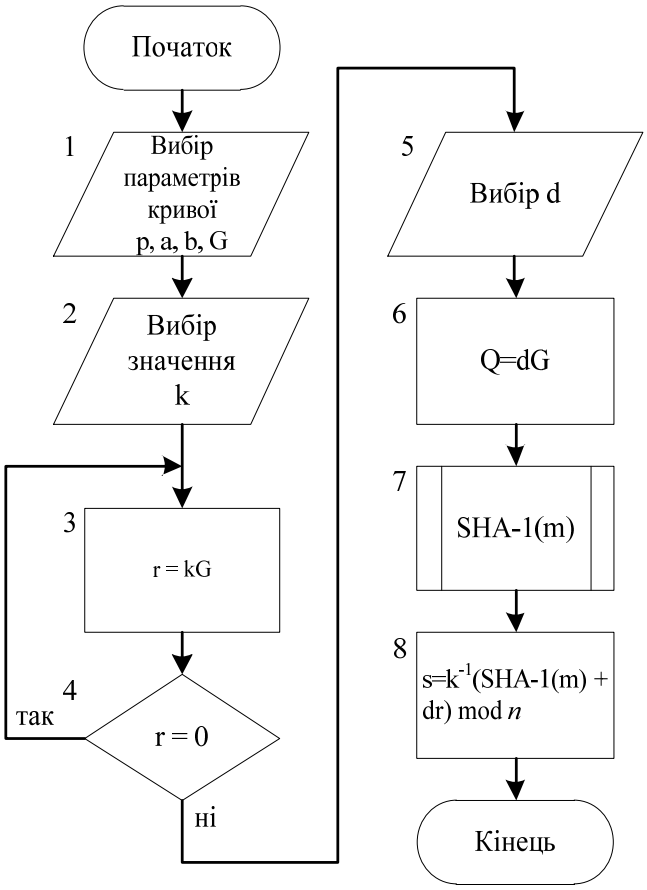

Рис. 5. Блок-схема реалізованого алгоритму постановки ЕЦП

На заміну даного алгоритму множення точки на число було використано наступний алгоритм. Для виконання операції множення точки P на число k послідовно знаходяться точки 2P, $2(2P) = 4P$, $2(4P) = 8P$, …, 2^iP,…, $2(2^{n-1}P) = 2^nP$, де n – кількість розрядів числа k у двійковому представленні. Точка kP знаходиться як сума тих точок 2^iP, для яких i-й розряд числа k у двійковому представленні рівний 1. Нехай двійкове представлення числа k містить r одиниць, тоді для виконання операції множення точки на число необхідно r - 1 операцій додавання та n - 1 операція множення точки на 2. У найгіршому для швидкодії випадку, коли r = n, необхідні n - 1 операція додавання та n - 1 операція множення точки на 2. Так як число n не перевищує $\log_2 k + 1$, досягається висока швидкість виконання операції множення точки на число. Блок-схема алгоритму множення точки на число представлена на рис. 6.

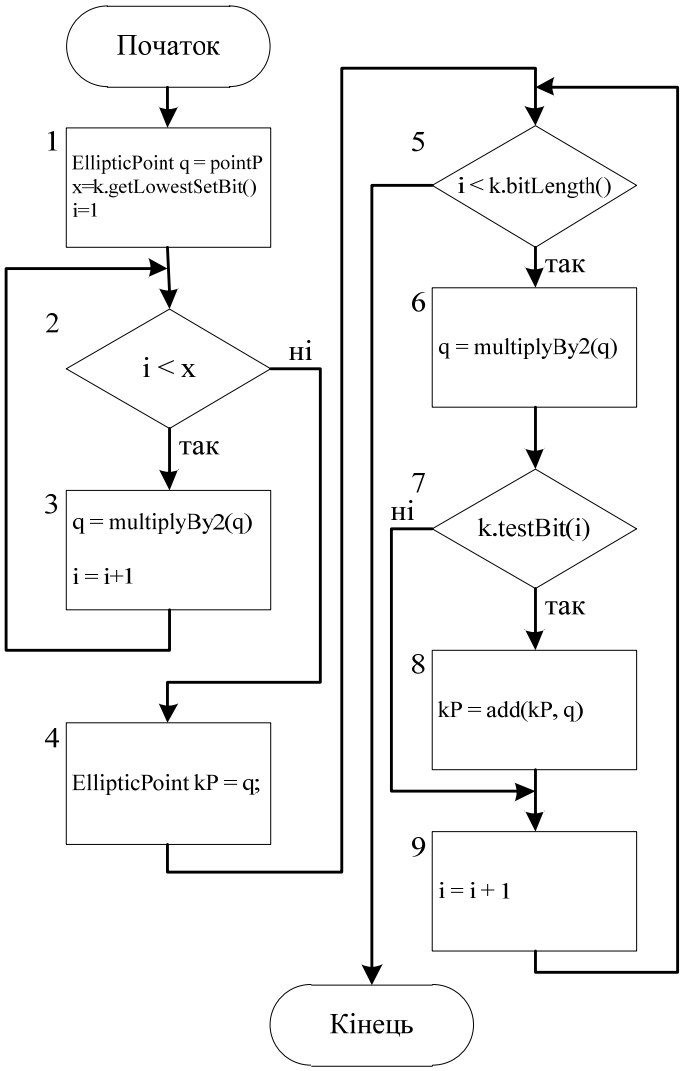

Рис. 6. Блок-схема алгоритму множення точки еліптичної кривої на число

6. Висновок

У даній роботі були досліджені сучасні схеми постановки електронного цифрового підпису та проведений порівняльний аналіз найбільш поширених схем.

В результаті дослідження схем постановки електронного цифрового підпису була отримана таблиця, у якій вказано розміри параметрів, що використовуються в обчисленнях, зберігаються на носіях а також передаються по каналам зв’язку. Згідно з отриманими результатами, алгоритм ECDSA при менших розмірах параметрів, що використовуються в обчисленнях та передаються по каналу зв’язку, здатен забезпечити більшу криптостійкість порівняно з іншими алгоритмами ЕЦП. Більша криптостійкість забезпечується завдяки використанню пробле-

ми знаходження дискретного логарифму в групі точок ЕК (яка аналогічна проблемі пошуку закритого ключа), для якої досі не знайдено алгоритму з реальним часом пошуку результату.

На основі алгоритму ECDSA реалізовано систему створення та верифікації ЕЦП на базі еліптичних кривих, що, на відміну від існуючих реалізацій, дозволяє варіювати параметри еліптичної кривої в широких межах, та надає засоби їх дослідження, серед яких побудова графіку точок еліптичної кривої з заданими параметрами, відображення результатів операцій над точками графіку, поетапне виконання постановки та верифікації ЕЦП, можливість використання суперсингулярних та аномальних еліптичних кривих для досліджень їх недоліків. Існуючі розробки були використані для створення учбового макету та програми для тестування знань в області еліптичних кривих та постановки ЕЦП. Також було досягнуте значне підвищення швидкості операції множення точки еліптичної кривої на число за рахунок використання покращеного алгоритму.

Порівняльний аналіз існуючих схем ЕЦП показав, що саме реалізований алгоритм підпису ECDSA є найбільш перспективним, так як довжина його ключа з підвищенням вимог до криптостійкості не так стрімко зростає, як у випадку інших існуючих алгоритмів, таких як RSA та DSA.

Список літератури

1. ДСТУ4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка, Київ: Держстандарт України, 2003.
2. Serge Vaudenay. A Classical Introduction to Cryptography: Applications for Communications Security, Springer, 2006.
3. D.Johnson and A.Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA), Univ. of Waterloo, 1999.
4. D.Johnson and A.Menezes. The Elliptic Curve Cryptosystem. Remarks on the security of the elliptic curve cryptosystem, Univ. of Waterloo, 2000.
5. Harold F. Tipton and Micki Krause. Information Security Management Handbook, Sixth Edition, 2006.