УДК 004.056.53(045) **DOI:** 10.18372/2310-5461.39.13091

А. В. Ільєнко**,** канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0001-8565-1117
e-mail: ilyenko.a.v@nau.edu.ua

С. С. Ільєнко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-0437-0995
e-mail: ilyenko.s.s@nau.edu.ua

ПРОГРАМНИЙ МОДУЛЬ З ВИКОРИСТАННЯМ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Вступ

Сьогодні в Україні активно розвивається інформаційне суспільство, однією з характеристик якого можна назвати орієнтацію на інтереси людей. У 1993 р. сутність інформаційного суспільства була розкрита Комісією ЄС: «Інформаційне суспільство — це суспільство, у якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку». В такому суспільстві кожний громадянин має можливість створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися та обмінюватися ними і, таким чином, реалізовувати свій у потенціал у сфері забезпечення особистого розвитку та підвищення якості життя.

Проблема збереження електронних документів від копіювання, модифікації і підробки потребує для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є електронний цифровий підпис, який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою. Програма електронного документообігу з використанням електронно-цифрового підпису (ЕЦП) на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Постановка завдання дослідження

Завданням даної роботи є характеристика теоретичних основ алгоритмів формування та верифікації ЕЦП з метою розробки програмного модуля для реалізації захисту інформаційних ресурсів, а саме забезпечення цілісності та конфіденційності інформації на базі удосконаленої схеми ДСТУ 4145-2002. Також проведення оцінювання ефективності отриманої модифікації алгоритму ДСТУ 4145-2002, що ґрунтується на перетвореннях в групі точок еліптичної кривої, з умови надання їй можливості відновлювати інформаційне повідомлення за допомогою обраного криптографічного алгоритму.

Теоретичні основи класифікації алгоритмів формування та верифікації ЕЦП

Існують різні класифікації сучасних схем електронного цифрового підпису. Їх можна класифікувати за механізмом побудови (симетричні та асиметричні), з відновленням повідомлення чи без, одноразові та багаторазові, детерміновані та ймовірнісні, за проблемою ,що покладена у їх основу.

Усі схеми ЕЦП також можна розділити на два великих класи: звичайні цифрові підписи (з доповненням) та електроні цифрові підписи з відновленням повідомлення. В ЕЦП з відновленням частина або повне повідомлення можуть бути відновленими з цифрового підпису, тобто для перевірки цифрового підпису необхідно знати тільки цифровий підпис та, можливо, сертифікат відкритого ключа. В ЕЦП з додаванням – цифровий підпис приєднується до повідомлення та зберігається і передається з ним, а для перевірки ЕЦП потрібно обов'язково мати сертифікат відкритого ключа [1].

Теоретичне обґрунтування та практичні дослідження ЕЦП з відновленням повідомлення були виконані, порівняно з ЕЦП з доповненням, пізніше. Значною мірою вони з'явилися, коли виникла необхідність в ЕЦП для коротких повідомлень. У 2003 р. був прийнятий міжнародний стандарт ISO/IEC 15946-4.

До нього було включено п'ять незалежних алгоритмів ЕЦП з відновленням повідомлення

(ECNR, ECMR, ECAO, ECPV, ECKNR), криптографічні перетворення в якому базуються на еліптичних кривих. У подальшому цей стандарт було удосконалено, і він був прийнятий в 2006 р. як ISO/IEC 9796-3 [2] на заміну існуючому. Стандарт IS0/IEC 9796-3 поширює й уточнює алгоритми, що вказані в IS0/IEC 15946-4, і з 2008 р. є основним стандартом підписів з відновленням повідомлення. Підписи мають спільну загальну схему Німберга–Руппеля, але в них використовують для оптимального використання *r*-компоненти модифікованого алгоритму передпідпису [3]. Додатково до нього був включений алгоритм ЕЦП, що ґрунтується на перетворенні в полі Галуа.

Схеми ЕЦП з відновленням повідомлення доцільно використовувати в інформаційних системах і протоколах з чітко визначеними повідомленнями. Це є принциповою особливістю з погляду їх застосування. Схема ЕЦП з відновленням повідомлення дає перевагу при застосуванні повідомлень невеликого розміру. Електронно-цифровий підпис, розроблений за такою схемою, може ефективно використовуватися в інфраструктурах з відкритими ключами, у протоколах з малим розміром повідомлення, наприклад, електронних магазинах для захисту товарів і послуг тощо.

Схеми з відновленням мають характерну особливість: зменшення розміру підпису за рахунок маскування у зворотній компоненті. Зменшення підпису має й негативні наслідки – підпис може мати менший розмір за рахунок зменшення збитковості, але це робить його потенційно більш вразливим до екзистенційної підробки.

Підпис з відновленням повідомлення, порівняно з підписом з доповненням, надає додаткову послугу безпеки — конфіденційність. Також для невеликих обсягів повідомлення можливо зробити таємною всю інформацію, що передається, у самому підписі. Відновити повідомлення можливо у разі відтворення передпідпису, що у загальному випадку можливо тільки при перевірці ЕЦП.

Таким чином, можна стверджувати, що повідомлення можна відновити лише за наявності відкритого ключа.

У відкритих системах така схема не має сенсу з надання послуг конфіденційності, але у разі, якщо циркуляція відкритих ключів в системі є контрольованою, є сенс у використанні цієї властивості схем з доповненням [4].

Окрім алгоритмів, зазначених в IS0/IEC 9796-3, до схем з відновленням інформаційного повідомлення належать схеми RSA, p-NEW, Zhang. Особливо необхідно відзначити, що усі підписи з відновленням повідомлення є асиметричними з погляду складності обчислення й перевіряння ЕЦП. Указане має бути враховано при обчисленні та перевірянні ЕЦП в реальному масштабі часу.

При порівнянні схем без відновлення повідомлення були виявлено, що алгоритми RSA та El-Gamal при однаковому розмірі ключа матимуть однакову криптостійкість (приблизно $2{,}7 \cdot 10^{28}$ для ключа 1024 біта). Але алгоритм El-Gamal є набагато швидшим за RSA при підписуванні документа, але поступається у швидкості при верифікації. Перевагою схеми El-Gamal є те, що при заданому рівні стійкості алгоритму цифрового підпису цілі числа, що беруть участь в обчисленнях, мають запис на 25 % коротше (в RSA множники повинні бути від 1024 біт, а в El-Gamal від 512 біт), що зменшує складність обчислень майже в два рази і дозволяє помітно скоротити обсяг використовуваної пам’яті. Крім того, процедура формування підпису за схемою El-Gamal не дозволяє обчислювати цифрові підписи під новими повідомленнями без знання секретного ключа. Проте схема El-Gamal поступається схемі RSA у неможливості відновлювати повідомлення та у тому, що довжина цифрового підпису в 1,5 рази більша, а це збільшує час її обчислення [6].

Перевагою алгоритмів DSA та ECDSA є менший розмір підпису, ніж в RSA та El-Gamal (у середньому 320 біт), тому що основні параметри системи мають розмірність 160 біт за замовчанням. Також при перевірці підпису більшість операцій з числами також проводиться за модулем числа довжиною 160 біт, що скорочує обсяг пам’яті і час обчислення [5]. Проте вважається, що ECDSA є більш криптостійким через складність проблеми дискретного алгоритмування по точках еліптичної кривої. Крім того, секретний ключ в ECDSA є унікальним, а не лише випадковим, як у DSA, що покращує надійність алгоритму. Алгоритм DSA має і недолік в тому, що він призначений лише для підписування/верифікації електронних документів, а не для їх шифрування/дешифрування, на відміну від усіх інших розглянутих алгоритмів. Але його перевагою може бути відносно нескладна реалізація та невелика затрата ресурсів.

Перевагою та особливістю схем з відновленням повідомлення є те, що наявна можливість не тільки переконатися у правдивості повідомлення, а ще й з тіла цифрового підпису автоматично отримати безпосередньо саме повідомлення. Це дозволяє ЕЦП зберігати не тільки цілісність переданого повідомлення, а й конфіденційність.. Схеми NR/ECNR зазвичай ефективні для роботи

з повідомлення невеликої довжини, тому що в такому випадку буде відновлюватися все повідомлення. Але варіант підписання великого повідомлення даними алгоритмами також передбачений, у такому випадку за допомогою збитковостей буде знаходитися частина повідомлення, що не зможе відновитися, і буде передаватися разом з підписом, а після перевірки ця та відновлене частина поєднаються, і можна буде отримати початкове повідомлення. Також дані алгоритми мають перевагу в криптостійкості та складності математичних проблем, на яких вони засновані. А застосування функцій знаходження збитковостей може гарантувати менші обсяги підпису на коротких повідомленнях. Окрім цього, завдяки тому, що схема ECNR діє з використання еліптичних кривих, це дає змогу використовувати параметри та ключі менших обсягів (а це оптимізує об'єм використовуваної пам'яті та збільшує швидкість при передачі даних). Саме тому найбільш ефективним та оптимальним був обраний алгоритм ECNR.

Сучасні схеми цифрового підпису можуть бути класифіковані відповідно до складної математичної проблеми, що лежить у їх основі та забезпечує їхню безпеку, а саме проблема дискретного логарифму в групі точок еліптичної кривої (ПДЛЕК); проблема дискретного логарифму (ПДЛ); проблема факторизації цілих чисел (ПФЧ).

За критерієм проблеми, що лежить в основі, можна зробити висновок, що найбільш криптостійкими будуть алгоритми, що ґрунтуються на ПДЛЕК.

До алгоритмів, заснованих на проблемі знаходження дискретного логарифму в групі точок еліптичної кривої над простим полем, можна віднести ECDSA, EC-KDSA, ECSS, ECNR.

У 2013 р. були досліджені та порівняні алгоритми, засновані на даних проблемах, для значення 10^{11} MIPS (величина, що показує число мільйонів інструкцій, які виконуються процесором за одну секунду під час деякого штучного тесту) років необхідних для злому закритого ключа [7]. Як порівнювальні характеристики, були взяті мінімальні ознаки, за яких реалізовується дана криптостійкість.

Результати порівняння зафіксовані в табл. 1.

Таблиця 1

Характеристики математичних проблем під час створення ЕЦП

Проблема,що лежить в основі алгоритму	ПФЧ	ПДЛ	ПДЛЕК
Розмір системних параметрів (біт)	1024	2208	481
Розмір підпису (біт)	1024	320	320
Розмір відкритого ключа (біт)	1088	1024	161
Розмір закритого ключа (біт)	2048	160	160

З цього випливає, що для того, щоб досягти нормального рівня безпеки при ПФЧ та ПДЛ необхідно використовувати ключ розміром 1024 біт, у той час як для алгоритму с ПДЛЕК достатньо ключа розміром 160 біт. Використання ключів меншої довжини зменшує кількість даних, які потребують обробки, зберігання та передачі по каналам зв'язку, а з поширенням технологій ЕЦП на мобільні пристрої, смарт-карти та інші пристрої з жорсткими обмеженнями обчислювальної спроможності, об'єму пам'яті та використовуваного трафіку, дана характеристика може стати вирішальною при виборі алгоритму ЕЦП. Крім того, було проаналізовано зміну розміру ключа відповідно до збільшення криптостікості. На рис. 1 можна побачити, що для алгоритмів з ПДЛЕК розмір ключа не так швидко та стрімко зростає, на відміну від алгоритмів з ПФЧ або ПДЛ.

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, оскільки невідомо алгоритму загального спрямування з субекспоненційним часом виконання. І крім того алгоритм з ПДЛЕК при менших розмірах параметрів, що використовуються в обчисленнях та передаються по каналу зв'язку, здатний забезпечити більшу криптостійкість порівняно з іншими алгоритмами ЕЦП.

Важливим є розгляд основного Державного стандарту України, який установлює механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$.

Необхідність його дослідження та подальшого використання полягає в тому, що саме в ньому встановлено механізм побудови ЕЦП та правила його застосування, які діють та застосовуються в більшості організацій та підприємств різних рівнів на території України.

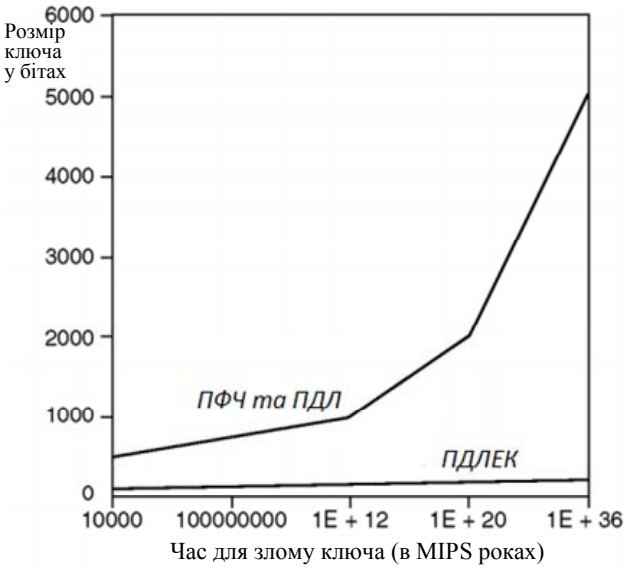

Рис. 1. Порівняння розмірів ключів відповідно до рівнів безпеки для різних схем створення ЕЦП

ДСТУ 4145-2002 (повна назва: «ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка») — національний стандарт України, що описує алгоритми формування та перевірки електронного цифрового підпису. Затверджено та надано чинності наказом Державного комітету Україні з питань технічного регулювання та споживчої політики від 28 грудня 2002 р. № 31.

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 [8, с. 6]. Стандарт гнучкий, стосовно вибору параметрів безпеки (наприклад, для нього можна обирати будь-яку функцію гешування, а не тільки ту, що зазначена в самому стандарті). Це дозволяє використовувати та підлаштовувати його майже під будь-яке апаратне та програмне середовище. Окремо треба відмітити те, що існують відкриті бібліотеки на мовах C/C++ та Java, у яких реалізовані основні криптопримітиви зі стандарту. Найбільшими перевагами є невеликий обсяг відкритого ключа (а це забезпечує досить швидку передачу та процес верифікації) та математична проблема, що покладена в основу механізму дії алгоритму. Найбільше переваг (висока криптостійкість та малі розміри параметрів) було знайдено в схемах з ПДЛЕК.

Модифікація стандарту ДСТУ 4145-2002 для надання йому можливості відновлювати інформаційне повідомлення за допомогою алгоритму ECNR

У попередній роботі було визначено теоретичні основи подальших шляхів удосконалення схеми ЕЦП відповідно до ДСТУ 4145-2002 з можливістю відновлення повідомлення, що дозволяє ввести додаткову послугу забезпечення конфіденційності та цілісності інформаційного повідомлення [9–12].

Обидва алгоритми ДСТУ 4145-2002 та ECNR засновані на математичній проблемі дискретного логарифмування в групі точок еліптичної кривої, а при детальному розгляданні можна побачити, що обидві схеми мають ще й майже однакову структуру. Тому алгоритм ECNR ідеально підходить для модифікації ДСТУ 4145-2002 та дана процедура потребувала мінімальних змін. Головною відмінністю стала заміна функції гешування на функцію маскування з використання геш-токену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з r-компоненти підпису.

Так, наприклад, загальні параметри цифрового підпису та спосіб їх формування є однаковими для обох алгоритмів.

Також незмінним буде обчислення ключової пари, тому даний етап повністю відтворюємо зі стандарту ДСТУ 4145-2002, а тому зобразимо їх на схемі (рис. 2).

Зауваження. У схемі не зазначено, але якщо поле задане поліноміальний базис, то необхідно зробити перевірку многочлена $f(t)$ на примітивність (перед перевіркою коефіцієнтів A та B)..

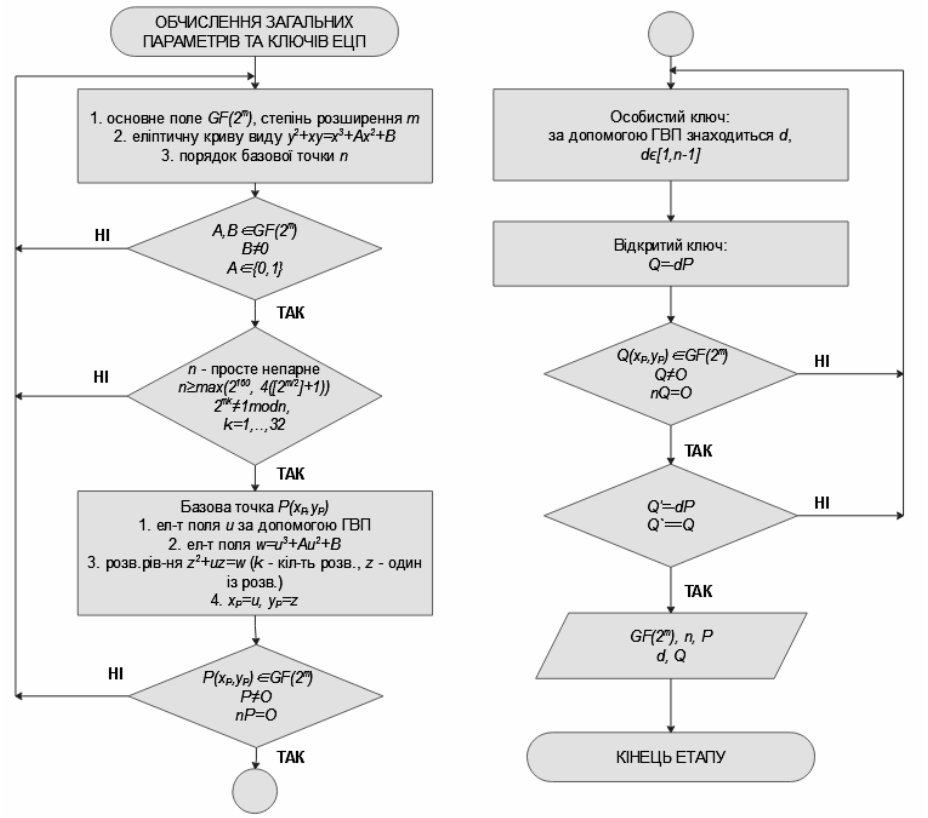

Рис. 2. Обчислення загальних параметрів ЕЦП та генерація ключової пари

По закінченню даного етапу маємо такі параметри: степінь розширення m; еліптична крива виду $y^3 + xy = x^3 + Ax^2 + B$; базова точка еліптичної кривої $P(x_P, Y_P)$; порядок базової точки n; закритий ключ d; відкритий ключ Q.

Етап формування підпису для модифікованого розглянемо детальніше. Зауважимо, що на відміну від звичайного ДСТУ 4145-2002 будемо використовувати не переведення параметрів до двійкового рядка, а їх перетворення на октети. Таким чином, будуть використовуватися такі функції: I2OSP — примітив перетворення цілих чисел в октетові рядки; OS2IP — примітив перетворення октетових рядків в цілі числа; EC2OSP — примітив перетворення еліптичної кривої в октетові рядки; OS2ECP — примітив перетворення октетових рядків в еліптичну криву.

Дані примітиви є обов'язковими складовими в бібліотеках для створення програмного забезпечення у сфері ЕЦП. Зручно одразу їх використовувати в описі наступних етапів, тому що вони будуть застосовані під час проектування програмного модуля. Повністю етап формування підпису зображений на рис. 3.

Отже, отриманий підпис має такі особливості, а саме в звичайному ДСТУ 4145 це (iH, M, D), хоч перший параметр і не обов'язковий,а при модифікації з відновленням отримуємо (M_{clr}, r, s), де M_{clr} буде використовуватися лише в одиничних випадках, а пара (r, s) і являє собою підпис D. Тобто, можна сказати, що при повідомленнях невеликої довжини, алгоритм з відновленням підпису буде ще й значно меншим за розміром порівняно з такими самими параметрами алгоритму без відновлення. Крім цього, після створення підпису запропонованим способом додається та забезпечується послуга конфіденційності даних, а також підвищується криптостійкість. Та необхідно вказати й недолік подібної модифікації — через додання математичних операцій (розщеплення повідомлення та його маскування) зменшується швидкість підписування.

Таким чином, відбувається модифікація ДСТУ 4145-2002 за допомогою алгоритму ECNR для надання йому функції відновлення повідомлення [9].

Це додає послугу конфіденційності, зменшує обсяг підпису, збільшує криптостійкість, проте сповільняє процедуру підпису/верифікації за однакових початкових параметрах.

Тепер можна перейти до верифікації підпису (рис. 4).

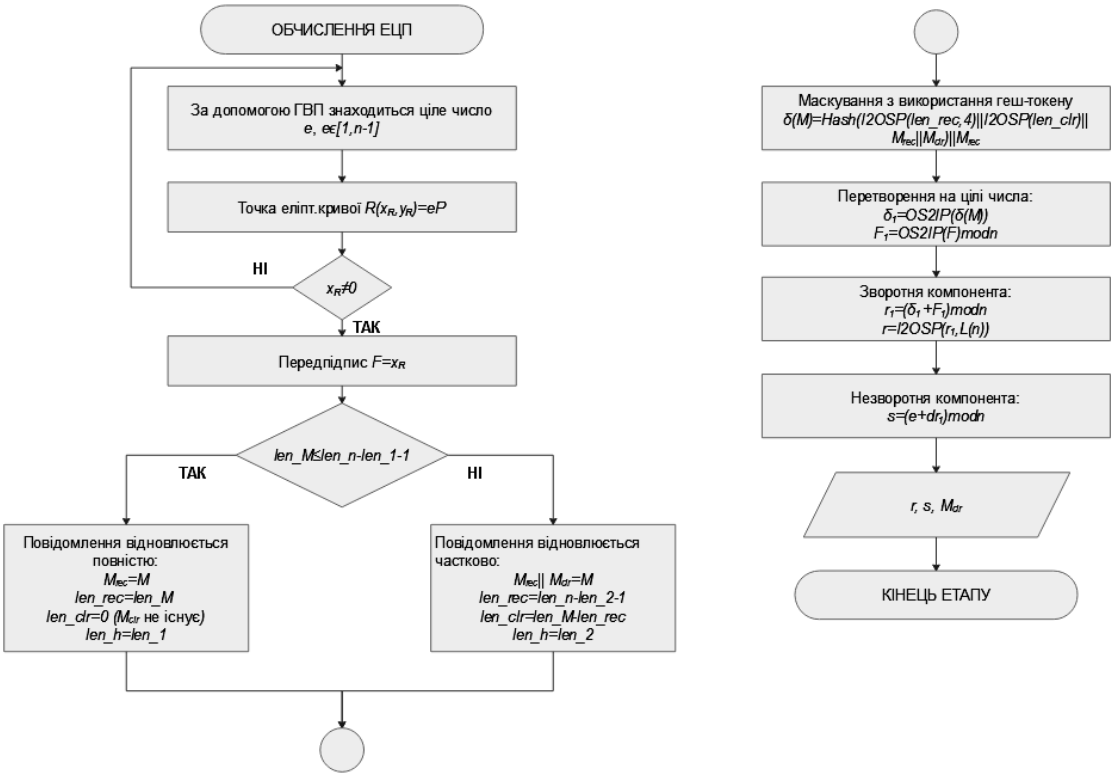

Рис. 3. Підписання повідомлення за модифікованим алгоритмом

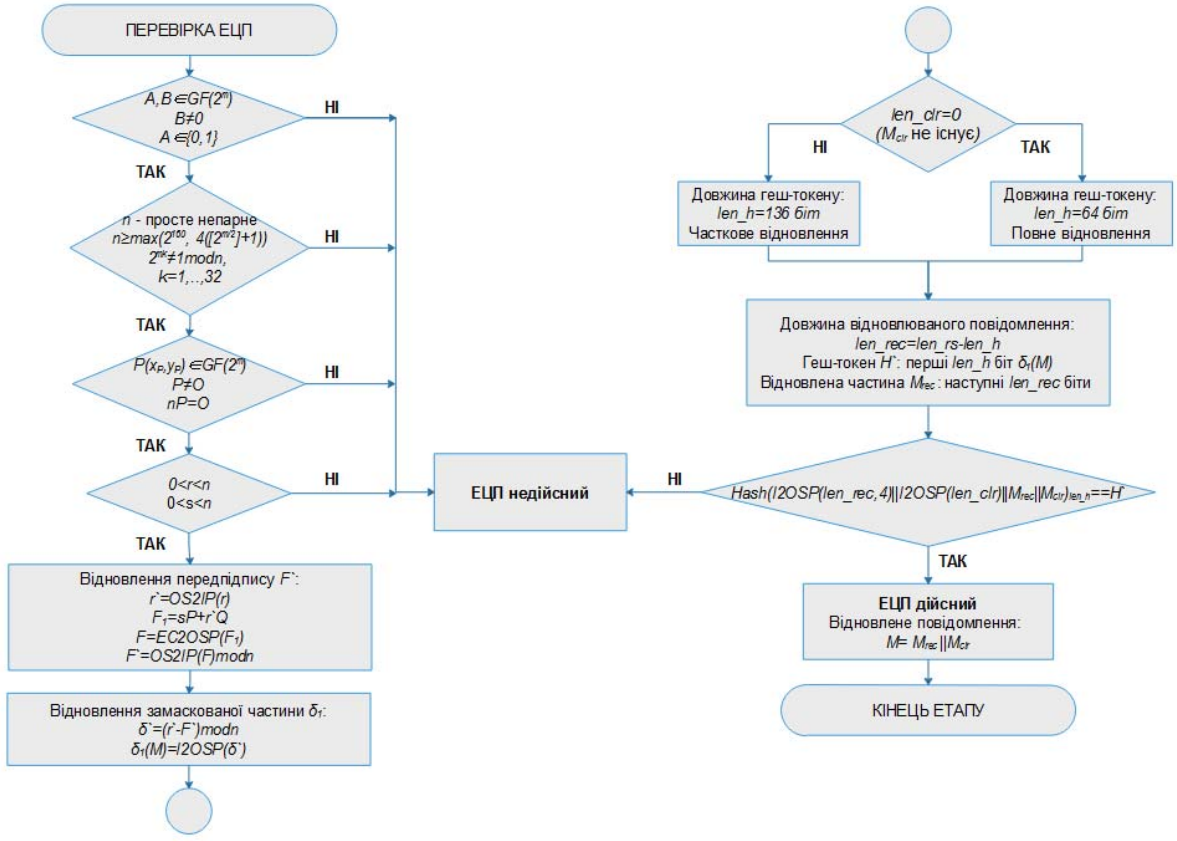

Рис. 4. Верифікація ЕЦП за модифікованим алгоритмом

Опис програмного модуля реалізації ЕЦП за Національним стандартом ДСТУ 4145-2002 з модифікацією на базі алгоритму ECNR, що заснована на проблемі дискретного логарифмування в групі точок еліптичної кривої

Програмний модуль створювався мовою C# та не накладає сертифікати, не використовує інфраструктуру відкритих ключів — вона призначена для роботи в невеликих локальних мережах. Тому вона виконує мінімум функцій: генерація ключів, їх зберігання, вибір документа та його підписання, проведення процедури верифікації, та в разі успіху — відновлення повідомлення.

Як пам'ятаємо, у ДСТУ 4145-2002 вказані еліптичні криві, які рекомендовані для подальшої роботи та їх характеристики. Тому зручно використовувати одну з них. Була обрана крива з поліноміального базису № 9. Ініціалізація еліптичної кривої та її параметрів показана далі в фрагменті коду:

```
int m = 367;
int k1 = 21;
int k2 = 0;
int k3 = 0;
var a = new BigInteger("1", 16);
var b = new BigInteger("43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE4
2CADAB8F93D92394C79A79755437B56995136", 16);
var n = new BigInteger("40000000000000000000000000000000000000000000000009C300B75A3FA824
F22428FD28CE8812245EF44049B2D49", 16);
var curve = new F2mCurve(m, k1, k2, k3, a, b) {N = n};
```

Усі функції, необхідні для роботи з еліптичними кривими, описані у файлі ECCurve.cs. Крім того, в файлах ECFieldElement.cs та ECPoint.cs описано роботу з елементами еліптичної кривої та базовою точкою відповідно.

Для генерації ключів було створено окремий файл, у якому містяться всі необхідні математичні операції та функції для створення відкритого та закритого ключів. Загальна функція генерації показана в фрагменті коду:

```
public static Key Generate(F2mCurve curve)
{
var basePoint = computeBasePoint(curve);
var privateKey =
= RNG.GetRandomInteger(curve.M);
var p1 = basePoint.Negate();
var publicKey =
= (F2mPoint)p1.Multiply(privateKey);
return new Key(curve, basePoint, publicKey,
privateKey);
}
```

Далі перед створенням ЕЦП необхідно сформувати передпідпис, що наведено далі в фрагменті коду:

```
public void computePreSignature()
{
while (true)
{
var e = RNG.GetRandomInteger(_key.Curve.M);
var r = _key.BasePoint.Multiply(e);
if (0 != r.X.ToBigInteger().SignValue)
{
_fe = (F2mFieldElement)r.X;
_e = e;
break;
}
}
}
```

Тепер можна підписувати вхідне повідомлення. Загальне використання функції створення ЕЦП можна побачити в фрагменті коду:

```
public BigInteger[] SignText(BigInteger h)
{
if (null == _key.PrivateKey)
throw new InvalidOperationException("null =
= _key.PrivateKey");
computePreSignature();
var h__element =
= new F2mFieldElement(_key.Curve.M,
_key.Curve.K1,
_key.Curve.K2, _key.Curve.K3, h);
var r = h__element.Multiply(_fe).ToBigInteger();
var s =
=_key.PrivateKey.Multiply(r).Add(_e).Mod(_key.
Curve.N);
return new[] { s, r };
}
```

Загальний варіант верифікації можна побачити в фрагменті коду:

```
public bool verifySignature(BigInteger h,
BigInteger s, BigInteger r)
{
var sP = _key.BasePoint.Multiply(s);
var rQ = _key.PublicKey.Multiply(r);
var r__ = sP.Add(rQ);
var h__element =
= new F2mFieldElement(_key.Curve.M,
_key.Curve.K1,
_key.Curve.K2, _key.Curve.K3, h);
var y2 = h__element.Multiply(r__.X);
if (y2.ToBigInteger().Equals(r))
return true;
return false;
}
```

Таким чином для підписання повідомлення необхідно лише обрати необхідний файл, який містить повідомлення, та параметри ключа (162, 256 або 512 біт). Програма автоматично згенерує ключі та підпише файл. У результаті користувач отримає файл *.key та *.sign з відкритим ключем та підписом відповідно. Для того, щоб перевірити ЕЦП, користувачеві необхідно мати файл з підписом та файл з відкритим ключем. Вони обидва є обов'язковими і в разі їх відсутності верифікації проводитися не буде. Якщо ж обидва файли обрані, то програма відтворює процедуру верифікації. У випадку вірності ЕЦП, користувачеві буде запропоновано відновити початкове повідомлення. При натисканні «Так» відкриється вікно, у якому міститиметься інформаційне повідомлення. Крім того було перевірено роботу програми у випадках зміни файлу *.sign або використанні іншого відкритого ключа. Як очікувалося, програма правильно реагує на подібні варіанти та сповіщає про недійсність ЕЦП.

Отже, було створено програмний модуль, який здатний підписувати повідомлення, формувати ключі та зберігати відкритий, перевіряти підпис, і в разі його вірності відновлювати інформаційне повідомлення. Це відбувається за алгоритмом ДСТУ 4145 з модифікаціями зі схеми ECNR, що заснована на проблемі дискретного логарифму в групі точок еліптичної кривої.

Оцінювання ефективності програмного модуля формування та верифікації ЕЦП на базі модифікованого алгоритму ДСТУ 4145-2002

Провівши необхідні операції для перетворення схеми ДСТУ 4145-2002 без відновлення повідомлення на схему з відновленням, можна провести їх аналіз та порівняти. Висновки та результати, отримані у попередньому підрозділі зафіксовано у табл. 2.

Таблиця 2

Порівняння звичайної та модифікованої схем ДСТУ 4145-2002

Параметри	ДСТУ 4145-2002	Модифікація ДСТУ 4145-2002
Забезпечення послуг	Цілісність	Цілісність Конфіденційність
Відновлення повідомлення	Ні	Так
Перетворення початкового повідомлення	Функція гешування	Функція маскування (+знаходження надлишковості)
Відкритий ключ, біт	163-768	112-768
Довжина підпису/Мінімальна довжина	Дайджест повідомлення + (r,s)/256 біт	(r,s) або (r,s,M_{clr})/162 біта
Час створення підпису, мс	1,24	1,98
Час перевірки підпису, мс	1,67	2,83

Отже, як можна побачити, разом з відновленням повідомлення модифікована версія ДСТУ 4145-2002 отримала змогу забезпечувати конфіденційність інформації, що передається. Також можна стверджувати, що у модифікованому варіанті можна використовувати відкритий ключ меншого розміру без загрози зменшення криптостійкості. Окрім цього, необхідно зазначити, що в разі повідомлення невеликої довжини (коли є можливість його повного відновлення), розмір підпису буде меншим і складатиметься всього з двох компонентів. Проте змінений алгоритм поступається звичайному у швидкості при однакових початкових параметрах. Та даний недолік не є критичним та звичайні користувачі майже не помітять зменшення швидкості підписання/верифікації.

Висновки

Отже, в статті була наведена повна характеристика модифікації Національного стандарту для створення та перевірки ЕЦП – ДСТУ 4145-2002 та знайдені його переваги та недоліки.

З огляду на те, що схеми ДСТУ 4145 та ECNR є схожими, обрана модифікація не потребувала значних змін.

Головна відмінність — заміна функції гешування на функцію маскування з використання геш-токену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з *r*-компоненти підпису.

Крім цього, було передбачено випадок підписання великого повідомлення, коли відновлюватися зможе тільки його частина.

Для цього було використано штучні збитковості повідомлення.

У результаті це додає схемі ДСТУ 4145-2002 послугу конфіденційності, зменшує обсяг підпису, збільшує криптостійкість, проте сповільняє процедуру підпису/верифікації за однакових початкових параметрах.

ЛІТЕРАТУРА

1. ISO/IEC 9796-3:2006: Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms, 2006. — URL:http://www.iso.org, doi.org/10.3403/30117202 (eng).

2. **Schneier B.** Applied cryptography: protocols, algorithms, and source code in C. — 2007, doi.org/10.1002/9781119183471 (eng).

3. **Горбенко Ю. І.** Аналіз властивостей та областей застосування цифрових підписів стандарту ISO/IEC 9796 – 3:2006 / Ю.І. Горбенко, А. А. Шевчук // Прикладная радиоелектроника. — 2009. — Т.8, №3. — С. 304–314.

4. **Шевчук А. А.** Особливості ЕЦП з відновленням повідомлення / А. А. Шевчук // Прикладная радиоэлектроника. — 2010. — Т.9, №3. — С. 489-492.

5. **Молдовян Д. Н.** Новый механизм формирования подписи в схемах ЭЦП, основанных на сложности дискретного логарифмирования и факторизации / Д. Н. Молдовян // Вопросы защиты информации. — 2005. — №4 (71). — С. 81–93.

6. **Алгулиев Р. М.** Исследование международных и национальных стандартов цифровой подписи на эллиптических кривых / Р. М. Алгулиев, Я. Н. Имамвердиев // Вопросы защиты информации. — 2005. — №2 (69). — С. 2–7.

7. **Полторак В. П.** Підвищення швидкодії процедури множення точки на число у алгоритмах електронного цифрового підпису на еліптичних кривих / В. П. Полторак, В. Б. Голков // Вісник НТУУ «КПІ»: Інформатика, управління та обчислювальна техніка. — К., 2013. — №57. — С. 155–163.

8. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. — К. : Держстандарт України, 2003.

9. **Ільєнко А. В.** Сучасні шляхи удосконалення процедури формування та верифікації електронно-цифрового підпису / А. В. Ільєнко, Г. О. Миронова // Наукоємні технології. — № 1 (37). — 2018. — С. 61–66, doi.org/10.18372/2310-5461.37.12370 (ukr).

10. **Чунарьова А. В.** Практичні схеми реалізації алгоритмів електронного цифрового підпису / А. В. Чунарьова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук.-техн. зб. — К. : НТУУ «КПІ», 2013. — № 1 (25). — С. 81–88.

11. **Ільєнко А. В.** Сучасні методи гомоморфного шифрування інформаційних ресурсів / А. В. Ільєнко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук; техн. зб. — К. : НТУУ «КПІ», 2015. — № 2 (30). — С. 52–57.

12. **Ільєнко А. В.** Оцінка ефективності оптимізованої криптосистеми Гентрі з умови забезпечення конфіденційності інформації / А. В. Ільєнко// Наукоємні технології. — № 1 (33). — 2017. — С. 41–45, doi.org/10.18372/2310-5461.33.11557(ukr).

Ільєнко А. В., Ільєнко С. С.

ПРОГРАМНИЙ МОДУЛЬ З ВИКОРИСТАННЯМ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

У статті проведено дослідження сучасних теоретичних основ класифікації алгоритмів формування та верифікації електронно-цифрового підпису. На основі проведеного аналізу та класифікації визначено, що в загальному за своєю структурою всі схеми електронно-цифрового підпису можна поділити на два великих класи: звичайні цифрові підписи (з доповненням) та електроні цифрові підписи з відновленням повідомлення. Проведені дослідження дозволили визначити, що схеми з відновленням повідомлення відрізняються від схем з доповненням тим, що вони не гешують повністю повідомлення, а замість них користуються функціями маскування та знаходження збитковостей повідомлення. Також визначено, що за критерієм проблеми, що лежить в основі формування та верифікації електронно-цифрового підпису, найбільш криптостійкими будуть алгоритми, що ґрунтуються на проблемі дискретного логарифму в групі точок еліптичної кривої. Також описаний підхід щодо забезпечення цілісності та конфіденційності інформації на основі ЕЦП на базі еліптичних кривих з використанням стандарту ДСТУ 4145-2002 та схеми Німберга–Руппеля, що надає можливість відновлення повідомлення. Головною відмінністю стала заміна функції гешування на функцію маскування з використання гештокену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з r-компоненти підпису. Описано програмний модуль реалізації електронно-цифрового підпису за національним стандартом ДСТУ 4145-2002 з модифікацією на базі алгоритму ECNR, що заснована на проблемі дискретного логарифмування в групі точок еліптичної кривої та проведено оцінювання ефективності програмної реалізації з умови забезпечення конфіденційності та цілісності.

Ключові слова: електронно-цифровий підпис, верифікація, конфіденційність, еліптичні криві, геш-токен, дискретне логарифмування

Ильенко А. В., Ильенко С. С.

ПРОГРАММНЫЙ МОДУЛЬ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕДУРЫ ФОРМИРОВАНИЯ И ВЕРИФИКАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В статье проведено исследование современных теоретических основ классификации алгоритмов формирования и верификации электронно-цифровой подписи. На основе проведенного анализа и классификации определено, что, в общем, по своей структуре все схемы электронно-цифровой подписи можно разделить на два больших класса: обычные цифровые подписи (с дополнением) и электронные цифровые подписи с восстановлением сообщения. Проведённые исследования позволили определить, что схемы с восстановлением сообщения отличаются от схем с дополнением тем, что они не хєшируют полностью сообщения, а вместо них пользуются функциями маскировки и нахождения избыточности сообщения. Также определено, что по критерию проблемы, лежащей в основе формирования и верификации электронно-цифровой подписи, наиболее криптостойкими будут алгоритмы, основанные на проблеме дискретного логарифма в группе точек эллиптической кривой. Также описан подход по обеспечению целостности и конфиденциальности информации на основе ЭЦП на базе эллиптических кривых с использованием стандарта ДСТУ 4145-2002 и схемы Нимберга-Руппеля, что даёт возможность восстановления сообщения. Главным отличием стала замена функции хеширования на функцию маскировки с использованием хэш-токена, что делает процедуру подписания и верификации обратными и даёт возможность восстанавливать сообщения с r-компоненты подписи. Описаны программный модуль реализации электронно-цифровой подписи с национальным стандартом ДСТУ 4145-2002 с модификацией на базе алгоритма ECNR, основанной на проблеме дискретного логарифмирования в группе точек эллиптической кривой и проведено оценивание эффективности программной реализации из условия обеспечения конфиденциальности и целостности.

Ключевые слова: электронно-цифровая подпись, верификация, конфиденциальность, эллиптические кривые, хэш-токен, дискретное логарифмирование

Ilyenko A. V, Ilyenko S. S

PROGRAM MODULE USING THE PROCEDURE FOR THE FORMATION AND VERIFICATION OF ELECTRONIC DIGITAL SIGNATURE

In the article the research of modern theoretical bases of classification of algorithms of formation and verification of electronic digital signature is carried out. Based on the analysis and classification, it has been determined that, in general, all electronic signature schemes can be divided into two large classes by their structure: ordinary digital signatures (with the addition) and electronic digital signatures with message recovery. The studies conducted have made it possible to determine that the message recovery schemes differ from the schemes with the addition that they do not completely hash the messages, but instead use the masking and redundancy features of the message. It is also determined that according to the criterion of the problem underlying the formation and verification of an electronic digital signature, algorithms based on the problem of a discrete logarithm in the group of points of an elliptic curve will be most crypto-resistant. Also described is the approach to ensuring the integrity and confidentiality of EDS-based information on the basis of elliptic curves using the standard DSTU 4145-2002 and the Niemberg-Ruppel scheme, which enables the recovery of the message. The main difference was the replacement of the hash function with the hash token function, which makes the signature and verification procedure reversed and allows you to retrieve messages from the signature r-component. The software module for implementing digital signatures with the national standard DSTU 4145-2002 with ECNR algorithm based on the problem of discrete logarithm in the group of points of the elliptic curve is described and the effectiveness of the software implementation from the condition of securing confidentiality and integrity has been evaluated.

Keywords: digital signature, verification, confidentiality, elliptical curves, hash token, discrete logarithm

Стаття надійшла до редакції 04.09.2018 р.
Прийнято до друку 18.09.2018 р.
Рецензент – д-р техн. наук, проф. Оксіюк О. Г.