УДК 004.056.53(045)
DOI: 10.18372/2310-5461.37.12370

А. В. Ільєнко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0001-8565-1117
e-mail: chunariova@gmail.com

Миронова Г. О.
Національний авіаційний університет
orcid.org/0000-0002-5407-7199
e-mail: mironcho.carpacho@gmail.com

СУЧАСНІ ШЛЯХИ УДОСКОНАЛЕННЯ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ

Вступ

Однією із форм створення, накопичення і обміну інформацією є система електронного документообігу.

Проте в даній системі існує загроза несанкціонованого доступу до інформації та, як наслідок, її нелегального копіювання, модифікації, видалення або розповсюдження.

Інструментом, що дозволяє створити правові основи для електронного документообігу (у тому числі в мережі Інтернет) та який може бути засобом захисту системи документообігу, є електронний підпис — дані в електронній формі, які додаються до інших електронних даних (електронних документів) або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Під поняттям електронно-цифрового підпису (ЕЦП) будемо розуміти вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача [1].

Постановка задачі дослідження

Завданням даної роботи є дослідження та порівняльний аналіз схем формування і верифікації ЕЦП з метою визначення подальших шляхів удосконалення схеми ЕЦП відповідно до ДСТУ 4145-2002 з можливістю відновлення повідомлення, що дозволить забезпечити конфіденційність та цілісність інформаційного повідомлення.

Аналіз існуючих алгоритмів формування та верифікації ЕЦП

В Україні основним документом, який регулює процедуру створення та перевірки ЕЦП є «ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» [2].

Все більшого поширення набувають системи ЕЦП, які дають можливість не тільки проводити верифікацію підпису, але й відновлювати початкове повідомлення з цифрового підпису. Це означає, що документ, який підписується, не буде передаватися відкритим каналом зв'язку, а буде складовою підпису, і перевіряючий його абонент отримає до повідомлення доступ лише в разі підтвердження авторства та цілісності. Таким чином, подібна структура ЕЦП забезпечує ще одну послугу безпеки — конфіденційність.

ДСТУ 4145-2002 не має здатності до відновлення повідомлення. Тому подальші дослідження будуть присвячені створенню системи для забезпечення цілісності, достовірності та конфіденційності інформації на основі ЕЦП на базі еліптичних кривих з використанням стандарту ДСТУ 4145-2002 з відновленням інформаційного повідомлення.

ДСТУ 4145-2002 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, с. 6].

До недоліків досліджуваного алгоритму можна віднести те, що механізм формування підпису та верифікації в самому стандарті досить складно описаний, тобто можуть виникнути труднощі з його розумінням та реалізацією. Крім того, в даному алгоритмі майже немає можливості розпаралелювання дій (тобто все повинно виконуватися лише послідовно) [3]. Також не можна сказати, що даний стандарт повсюдно використовується на території України — чимало організацій та підприємств використовують російські або американські стандарти.

Проте переваг даний стандарт має більше. По-перше, завдяки тому, що він прийнятий на державному рівні, то має юридичну силу в Україні та є повністю законним. По-друге, стандарт гнучкий стосовно вибору параметрів безпеки (наприклад, для нього можна обирати будь-якому 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. Та 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. Стандарт заснований на математичній проблемі знаходження дискретного логарифму в групі точок еліптичної кривої (ПДЛЕК). І давно відомо, що алгоритми, що базуються на цій основі, мають більшу криптостійкість при відносно малих параметрах, на відміну від алгоритмів, які спираються на проблему факторизації чисел (ПФЧ) та проблему дискретного логарифмування в кінцевому полі (ПДЛ). Детальніше це зображено в таблиці, у якій наведені їх значення для різних алгоритмів.

Порівняння характеристик алгоритмів

Алгоритм	Проблема в основі	Відкритий ключ, біт
ДСТУ 4145-2002	ПДЛЕК	163-768
DSA	ПДЛ	1024-3072
ECDSA	ПДЛЕК	112-570
RSA	ПФЧ	512-4096

Схема ЕЦП ДСТУ 4145-2002 належить до схем з доповненням повідомлення, проте існують і схеми з відновленням. 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 [4; 6].

Структурно схеми с відновленням повідомлення відрізняються від схем з доповненням тим, що вони не гешують повністю повідомлення (проте в різних алгоритмах частково можуть використовуватися геш-функції), а замість них користуються функціями маскування та знаходження збитковостей повідомлення. Такий алгоритм має свої переваги:

– користувач, який верифікує підписане повідомлення, отримає до нього доступ лише в разі підтвердження дійсності підпису;

– окрім забезпечення цілісності повідомлення, може ще й забезпечувати його конфіденційність;

– ЕЦП з відновленням може забезпечувати менший обсяг підпису при невеликих повідомленнях;

– обов'язкове використання функцій формування збитковості повідомлення (етап створення передпідпису), що надає гнучкий функціонал (наприклад, обираючи тип збитковості, можна визначити, чи буде відновлена частина повідомлення або повністю усе повідомлення), а також підвищує криптостікість.

До алгоритмів заснованих на даній схемі можна віднести RSA, NR (схема Німберга-Руппеля) та її модифікація на еліптичних кривих ECNR, а також Zhang, ECMR, ECAO, ECPV, ECKNR.

Алгоритм RSA має переваги в тому, що він є найбільш поширеним, має високі показники швидкості під час підписання/верифікації, а також є універсальним, тому що ще й придатний для шифрування/дешифрування. Схеми NR на відміну від RSA зазвичай ефективні для роботи з повідомлення невеликої довжини, тому що в такому випадку буде відновлюватися все повідомлення. Проте дані алгоритми мають перевагу в криптостійкості та складності математичних проблем, на яких вони засновані. 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 вико-

ристовуваної пам'яті та збільшує швидкість при передачі даних). Саме тому найбільш ефективним та оптимальним для подальшого моделювання є алгоритм ECNR, і буде використовуватися його схема, наведена в міжнародному стандарті IS0/IEC 9796-3 [5].

При детальному розгляданні можна побачити, що обидві схеми, ДСТУ 4145-2002 та ECNR, мають майже однакову структуру. Тому алгоритм ECNR ідеально підходить для удосконалення ДСТУ 4145 та дана процедура потребуватиме мінімальних змін. Як і всі схеми ЕЦП, ця складається з 3-х основних етапів.

Знаходження загальних параметрів цифрового підпису та генерація ключів

Загальні параметри обираються так:

– вибір основного поля GF(2m). У тексті стандарту наведені рекомендовані значення степені поля m при поліноміальному та нормальному базисах;

– вибір еліптичної кривої вигляду

$$y^3 + xy = x^3 + Ax^2 + B, \quad (1)$$

де коефіцієнти рівняння A, $B \in GF(2m)$, $B \neq 0$, $A \in \{0,1\}$. Дані коефіцієнти дозволено й рекомендовано брати з додатку Г стандарту.

Обчислення базової точки еліптичної кривої P. Для цього необхідно виконати такі кроки:

1) обчислити випадковий елемент u основного поля за допомогою генератор випадкових послідовностей (ГВП) (описаний в додатку А стандарту);

2) обчислити елемент основного поля $w = u^3 + Au^2 + B$;

3) розв'язати рівняння $z^2 + uz = w$ (необхідно отримати кількість розв'язків рівняння k та один із розв'язків z);

4) $x_P = u$, $y_P = z$. Координати (x_P, y_P) описують шукану базову точку еліптичної кривої P.

Знаходження порядку базової точки P: n має бути непарним цілим числом, $n \geq \max(2^{160}, 4([2^{m/2}] + 1))$. Окрім того має виконуватися умова $2^{mk} \neq 1 \bmod n$ при $k = 1,..,32$.

Ключі обчислюють стандартним для еліптичних кривих способом:

– особистий ключ d знаходять за допомогою ГВП, при чому $d \in [1, n-1]$;

– відкритий ключ можна обчислити, як $Q = -dP$. Координати точки $Q(x_Q, y_Q)$ мають належати $GF(2^m)$ та бути розв'язком рівняння (1), $Q \neq O$ (O — нескінченно віддалена точка еліптичної кривої), $nQ = O$.

Формування підпису повідомлення

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 на цілі числа;
- *EC2OSP* — примітив перетворення еліптичної кривої в октетові рядки;
- *OS2ECP* — примітив перетворення октетових рядків в еліптичну криву.

Випадковий параметр та передпідпис обчислюються без змін. Тобто знаходять випадкове число e ($e \in [1; n-1]$), точка еліптичної кривої $R(xR, yR) = eP$ (обов'язково перевірити, що $xR \neq 0$) та передпідпис $F = xR$.

І після цього моменту вже будуть поширюватися зміни з алгоритму ECNR. У попередніх розділах було вказано, що схеми за Німберг–Руппелем мають недолік в тому, що не завжди можуть відновити все повідомлення.

Відновлення відбувається повністю, якщо повідомлення відносно невеликої довжини. І хоч в роботі не будуть використовуватися повідомлення великого обсягу, але варіант для них все одно треба обов'язково описати.

Для цього початкове повідомлення M необхідно розщепити на дві частини: M_{rec} — частина, що відновлюється та M_{clr} — частина, що надсилається (це означає, що M_{clr} буде додаватися до підпису при передачі даних). Тобто, можна сказати, що $M = M_{rec} || M_{clr}$, і надалі також будуть використовуватися їх довжини *len_M*, *len_rec* та *len_clr* відповідно (зрозуміло, що *len_M* = *len_rec*+*len_clr*).

При роботі з ЕЦП з відновленням повідомлення доцільно використовувати збитковість. В цьому випадку зручно обрати коротку та довгу збитковості та прийняти їх значення як *len_1 = 64 біта* та *len_2 = 136 бітів* (мінімальні значення за стандартом ISO/IEC 9796-3). Тепер можна провести перевірку умови

$$len\_M \leq len\_n - len\_1 - 1, \quad (2)$$

і якщо вона виконується, тоді можна бути впевненим, що повідомлення буде відновлене повністю.

Тобто це означає, що $M_{rec} = M$, *len_rec* = *len_M*, *len_clr* = 0 (M_{clr} не існує) та *len_h* = *len_1* (довжина результату геш-токену).

Якщо ж умова (2) не виконується, тоді приймається, що *len_rec=len_n-len_2-1, len_clr = len_M-len_rec* та *len_h=len_2*. У такому разі маємо частину, що не відновлюється та буде відсилатися разом з підписом M_{clr}.

Згідно зі стандартом ISO/IEC 9796-3 для алгоритму ECNR та NR для маскування обчислюється геш-токен частини, що відновлюється

$$\delta(M) = Hash(I2OSP(len\_rec,4)||I2OSP(len\_clr)|| ||M_{rec}||M_{clr})||M_{rec}, \quad (3)$$

де як функцію хешування використовують ГОСТ 34.311, тому що саме вона рекомендована ДСТУ 4145. При цьому у випадку повного відновлення повідомлення використовуються тільки перші 64 біти отриманого дайджесту, а при частковому відновленні — перші 136 бітів.

Далі необхідно перетворити результат геш-токену та передпідпис на цілі числа: $\delta_1 = OS2IP(\delta(M)$ та $F_1 = OS2IP(F)modn$.

Тепер можна перейти безпосередньо до обчислення підпису. Спочатку вираховується зворотна компонента r: $r_1 = (\delta_1 + F_1)\ modn$ та $r = I2OSP(r_1, L(n))$.

А незворотна компонента знаходиться як $s = (e + dr_1)modn$.

Таким чином, передаватися будуть пара чисел (r, s) (при бажанні їх можна перетворити на цифровий рядок згідно ДСТУ 4145-2002) та частина повідомлення M_{clr} в разі часткового відновлення повідомлення.

Можна зробити перші висновки. Не дивлячись на те, що структурно алгоритми ДСТУ 4145-2002 та ECNR дуже схожі, проте в ДСТУ 4145-2002 обов'язково використовується функція гешування для знаходження дайджесту повідомлення. Проте вона робить не можливим подальше відновлення повідомлення, тому в даній частині використовувалася функція зі схеми Німберг–Руппеля. Для того, щоб мати змогу відновлювати повідомлення, також було додано можливість розчепити його на дві частини та додана умова перевірки довжини повідомлення відповідно до порядку базової точки еліптичної кривої та короткої збитковості (значення встановлене за замовченням).

Замість геш-функцій обчислюється функція маскування з використанням геш-токену. Хоч в даному випадку і знаходиться дайджест гешування, проте він є не остаточним результатом, а компонентом, що приєднується до передаваємої частини повідомлення, таким чином маскуючи її.

Також для знаходження зворотної компоненти підпису використовується скалярне складання замість скалярного множення (для надання зворотності підпису та подальшого відновлення).

Верифікація підпису

Спочатку рекомендується зробити стандартну перевірку загальних базових параметрів та відкритого ключа:

1. Степінь розширення поля m повинна бути обрана з таблиць ДСТУ 4145-2002 (а при поліноміальному базисі ще й необхідно виконати перевірку на примітивність).

2. Перевірка рівняння еліптичної кривої і порядку базової точки. Коефіцієнти еліптичної кривої повинні задовольняти вимогам: A, $B \in GF(2m)$, $B \neq 0$, $A \in \{0,1\}$. Порядок базової точки n має бути непарним цілим числом, $n \geq \max(2160, 4([2m/2]+1))$. Окрім того, має виконуватися умова $2mk \neq 1 \bmod n$ при $k = 1,..,32$.

3. Перевірка базової точки. Координати xP, $yP \in GF(2m)$ та є розв'язком рівняння (1), $P \neq O$ (O — нескінченно віддалена точка еліптичної кривої), $nP = O$.

3. Перевірка відкритого ключа. Координати xQ, $yQ \in GF(2m)$ та є розв'язком рівняння (1), $Q \neq O$ (O — нескінченно віддалена точка еліптичної кривої), $nQ = O$.

Також необхідно перевірити складові підпису: $0 < r < n$ та $0 < s < n$. Якщо хоч одна з усіх цих вимог не виконується, то підпис вважається недійсним.

Далі октетовий рядок r перетворюється на ціле число: $r` = OS2IP(r)$. Та відновлюється передпідпис $F_1 = sP + r`Q$, перетворюється в октетові рядки $F = EC2OSP(F_1)$, а потім в ціле число $F` = OS2IP(F)modn$.

Після цього відновлюється замаскована частина підпису $\delta` = (r` - F`)modn$ і перетворюється в октетові рядки $\delta_1(M) = I2OSP(\delta`)$. Таким чином ми отримуємо рядок, який складається з геш-токену та початкового повідомлення.

Далі проводиться наступний аналіз: якщо в частині отриманого підпису було три компоненти, тобто був параметр M_{clr}, тоді робиться висновок, що повідомлення не повністю відновлюється, а значення збитковості буде складати 136 біт. Якщо M_{clr} відсутнє, тоді повідомлення відновлюється повністю, а його збитковість складає 64 біта.

Очевидно, що результат геш-токену len_h — це перші збиткові біти $\delta_1(M)$, які ми позначимо як $H`$. Це значить, що всі наступні біти — і є передаваємим повідомленням M_{rec}. Тепер необхідно зробити повторне маскування. У нашому випадку ми вже маємо M_{rec} та M_{clr} та знаємо їх довжини і робимо перевірку:

$$Hash(I2OSP(len\_rec,4)||I2OSP(len\_clr)||M_{rec}|| || M(_{clr})_{len\_h} = H`. \quad (4)$$

Якщо рівність вірна, то підпис верифікований, а відновленим повідомленням є $M = M_{rec}\ ||M_{clr}$. Якщо рівність не підтверджується, то підпис вважається не дійсним і повідомлення не відновлюється.

Тож можна зробити висновок і про зміни в процедурі перевірки підпису. Без змін залишився етап перевірки загальних параметрів та відкритого ключа.

Процедура верифікації у ДСТУ 4145-2002 з відновленням повідомлення відрізняється в першу чергу, видом підпису (саме повідомлення не передається, воно є складовою частиною компоненти *r*).

У варіанті з відновленням повідомлення передається пара (*r*, *s*) — октетовий рядок та ціле число, а в стандартному вигляді це один рядок *D*, проте ці дані взаємопов'язані та є одним і тим самим значенням, представленому у різних виглядах (просто для алгоритмів з відновленням встановлено такий тип запису, саме тому він і був обраний). Далі передпідпис відновлюється абсолютно однаково. Проте відбувається зміна самого принципу остаточної перевірки. Якщо в стандартному варіанті алгоритму знаходиться *r`* та перевіряється з отриманою з підпису *r*-компонентою, то алгоритм з відновленням потребує більше дій. Після знаходження замаскованого повідомлення, треба відділити його від «маски» (геш-токену), обчислити геш-токен зі знайденими значеннями, і тільки після цього можна робити порівняння.

Також важливою відмінністю є те, що в звичайному варіанті алгоритму порівнюються цілі числа, а в випадку з відновленням, результати маскування, тобто аналізується семантичне значення.

Теж саме відбувається з удосконаленням ДСТУ 4145-2002 за допомогою алгоритму ECNR для надання йому функції відновлення повідомлення. Це додає послугу конфіденційності, зменшує обсяг підпису, підвищується криптостійкість. Проте необхідно сказати, що додаткові математичні операції, які були використані у схемі з відновленням повідомлення, можуть значно сповільняти процедуру підпису/верифікації при однакових початкових параметрах порівняно зі звичайним алгоритмом ДСТУ 4145-2002.

Висновки

У даній статті описані теоретичні основи реалізації удосконаленої схеми ДСТУ 4145-2002, якій була надана можливість відновлення інформаційного повідомлення за допомогою алгоритму ECNR, що заснований на проблемі дискретного логарифмування в групі точок еліптичної кривої. Це додає послугу конфіденційності, зменшує обсяг підпису, збільшує криптостійкість, проте сповільняє процедуру підпису/верифікації через додаткові математичні операції за однакових початкових параметрах.

ЛІТЕРАТУРА

1. Закон України «Про електронний цифровий підпис» № 852-IV від 22.05.03: зі змінами внесеними згідно із Законом України № 222-VIII від 02.03.2015 [Електронний ресурс]. — Режим доступу: http://zakon3.rada.gov.ua/laws/show/851-15

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

3. **Болтьонков В. О., Єнікєєв Р. І.** Практичне дослідження сучасних систем електронного цифрового підпису / В. О. Болтьонков, Р. І. Єнікєєв // Інформатика та математичні методи в моделюванні. — 2014. — Т. 4, №3. — С. 201–209.

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

5. 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)

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

Ільєнко А. В., Миронова Г. О.

СУЧАСНІ ШЛЯХИ УДОСКОНАЛЕННЯ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ

У статті проведено порівняльний аналіз існуючих алгоритмів формування та верифікації електронно-цифрового підпису, а саме визначено найпоширеніші алгоритми та проведено критеріальне порівняння за математичними основами на яких заснований алгоритм та розмірами значення відкритого ключа. На основі проведеного аналізу визначено, що існують схеми з доповненням повідомлення та схеми з відновленням інформаційного 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. Було визначено, що найбільш ефективним та оптимальним для подальшого використання є схема Німберга–Руппеля, яка заснована на базі еліптичних кривих (ECNR). В статті описані теоретичні основи створенню системи для забезпечення цілісності, достовірності та конфіденційності інформації на основі ЕЦП на базі еліптичних кривих з використанням стандарту ДСТУ 4145-2002 з можливістю відновленням інформаційного повідомлення на базі ECNR.

Ключові слова: електронно-цифровий підпис; верифікація; конфіденційність; еліптичні криві.

Ilyenko A. V., Mironova A. A.

MODERN WAYS OF IMPROVING THE PROCEDURE FOR THE FORMATION AND VERIFICATION OF DIGITAL SIGNATURE

In the article, a comparative analysis of existing algorithms for the formation and verification of the digital signature has been carried out, namely, widespread algorithms and the criteria for comparison was the mathematical basics on which the algorithm is based and the size of the public key. Based on the analysis, it is established that there are schemes with the addition of messages and schemes with the restoration of the information message. The conducted studies made it possible to determine that the schemes with message recovery differ from the schemes with the addition that they do not completely hash messages, but instead use masking functions and redundancy of the message. It was determined that the most effective and optimal for further use is the Nimberg-Ruppel scheme, which is based on elliptical curves (ECNR). The article describes the theoretical basis for creating a system for ensuring the integrity, reliability and confidentiality of information based on digital signatures based on elliptical curves using the standard DSTU 4145-2002 with the possibility of restoring an information message based on ECNR.

Keywords: digital signature; verification; confidentiality; elliptical curves.

Ильенко А. В., Миронова А. А.

СОВРЕМЕННЫЕ ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРОЦЕДУРЫ ФОРМИРОВАНИЯ И ВЕРИФИКАЦИИ ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ

В статье проведён сравнительный анализ существующих алгоритмов формирования и верификации электронно-цифровой подписи, а именно определено распространённые алгоритмы и проведения критериальное сравнения по математическим основами на которых основан алгоритм и размерами значение открытого ключа. На основе проведённого анализа установлено, что существуют схемы с дополнением сообщения и схемы с восстановлением информационного сообщения. Проведённые исследования позволили определить, что схемы с восстановлением сообщения отличаются от схем с дополнением тем, что они не хешируют полностью сообщения, а вместо них пользуются функциями маскировки и нахождения избыточности сообщения. Было определено, что наиболее эффективным и оптимальным для дальнейшего использования является схема Нимберга–Руппеля, которая основана на базе эллиптических кривых (ECNR). В статье описаны теоретические основы созданию системы для обеспечения целостности, достоверности и конфиденциальности информации на основе ЭЦП на базе эллиптических кривых с использованием стандарта ДСТУ 4145-2002 с возможностью восстановлением информационного сообщения на базе ECNR.

Ключевые слова: электронно-цифровая подпись; верификация; конфиденциальность; эллиптические кривые.

Стаття надійшла до редакції 22.02.2018 р.
Прийнято до друку 23.02.2018 р.
Рецензент — д-р техн. наук, доц. Корнієнко Б. Я.