УДК 681.3.06

К.А. ПОГРЕБНЯК, канд. техн. наук, Ю.М. ЛЄНШИНА

СХЕМА ХАМЕЛЕОН-ПІДПИСУ НА ОСНОВІ ДСТУ 4145-2002

Вступ

Стрімкий розвиток систем, що пов'язані з електронною комерцією (наприклад, інтернет-аукціони або системи закритого електронного голосування), призвів до необхідності додаткових послуг безпеки. Окрім традиційних послуг цілісності та неспростовності, які забезпечує звичайний механізм електронного цифрового підпису (ЕЦП), виникла необхідність забезпечення послуг приватності. За приватністю у даному контексті слід розуміти непередаваність ЕЦП та прихованість підписаного повідомлення. Непередаваність ЕЦП – неможливість доведення валідності ЕЦП будь-якій третій стороні без участі підписувача. Прихованість повідомлення – відсутність необхідності розкриття підписувачем змісту підписаного повідомлення у ході виникнення можливих протиріч. Ці послуги забезпечує механізм хамелеон-підпису, який представляє собою довільний базовий алгоритм ЕЦП із застосуванням геш-функції спеціального виду – функції геш-хамелеону.

Як відомо, у якості легітимної системи ЕЦП в Україні працює інфраструктура відкритих ключів, що використовує у якості стандарту ЕЦП – ДСТУ 4145-2002. Метою наших досліджень є розробка алгоритму ЕЦП, що, з однієї сторони, зміг би забезпечити необхідні послуги, а з іншої – не суперечив би діючим нормативним документам і мав би використовуватися в існуючій інфраструктурі відкритих ключів. У статті пропонується механізм хамелеон-підпису на основі ДСТУ 4145-2002, що задовольняє висунутим вимогам.

1. Історичний аналіз розвитку хамелеон-підписів

Механізм хамелеон-підпису, що вперше був представлений у роботі Кравчука та Рабіна [1], базується на звичній парадигмі геш-та-підпис, де функція геш-хамелеону використовується для обчислення криптографічного дайджесту повідомлення. Функція геш-хамелеону представляє собою односторонню геш-функцію, яка не дозволяє нікому, окрім власника інформації про лазівку, обчислити колізію для випадково обраних вхідних даних. Хамелеон-підпис є неінтерактивним, тобто підписувач може згенерувати хамелеон-підпис без попереднього зв'язку з визначеним одержувачем, і одержувач, в свою чергу, може перевірити валідність підпису без взаємодії з підписувачем. З іншої сторони, якщо створено підроблений підпис, підписувач може заперечувати його дійсність шляхом відкриття деяких значень, але не змісту повідомлення (прихованість повідомлення). Протокол спростування підробленого підпису також є неінтерактивним. Суттєвим обмеженням оригінального алгоритму хамелеон-підпису є те, що результатом підробки підпису є знаходження підписувачем інформації про лазівку, якою володіє одержувач, тобто його секретного ключа [2]. Підписувач може використати цю інформацію з метою заперечення валідності інших підписів, які він раніше підписував для цього одержувача. У гіршому випадку підписувач має можливість зв'язатися із зловмисною метою з іншими учасниками інформаційного обміну для заперечення валідності інших підписів, що перевіряються однаковим відкритим ключем. Хоча це стримує одержувача від підробки ЕЦП, у багатьох застосуваннях таке обмеження є неприпустимим. Пізніше ця проблема отримала назву проблеми витоку ключа. Атеніс та Медейрос [2] вперше запропонували вирішення проблеми витоку ключа шляхом застосування криптографії, що базується на ідентифікаторах. Тепер підписувач зміг підписувати повідомлення визначеному одержувачу без попереднього запиту його сертифіката відкритого ключа (СВК). Більш того, підписувач використовує різні відкриті ключі (пов'язані з різними секретними ключами) для кожної транзакції з одержувачем. Таким чином, результатом створення підробленого підпису може бути лише відкрита підписувачем інформація про лазівку, пов'язана з конкретною транзакцією. Але ця схема не отримала широкого застосування, адже разом з вирішенням проблеми витоку ключа виникла проблема розповсюдження дуже великої кількості ключів (для кожної транзакції свій відкритий, а отже і секретний ключ), вирішення якої, як відомо, є складною задачею.

У роботі Чена [3] вперше з'явилася ідея створення геш-хамелеона, вільного від проблеми витоку ключа, що заснована на використанні гап-груп Діффі-Гелмана (GDH groups – Gap Diffi-Helman groups) з білінійними спарюваннями. Потім Атеніс і Медейрос [4] представили три схеми хамелеон-підписів, вільні від проблеми витоку ключа, дві з яких засновані на припущеннях RSA (вперше схеми не застосовували спарювання), а третя – на спарюваннях. Пізніше Гао [5] представив схему хамелеон-підпису, вільну від проблеми витоку ключа, що базувалася на схемі підпису Шнора. Однак вона потребувала інтерактивного зв'язку між підписувачем і одержувачем, що підривало концепцію неінтерактивності хамелеон-підпису.

Усі існуючи схеми геш-хамелеонів, що базувалися на складності вирішення задачі дискретного логарифму, могли бути реалізовані лише у GDH групах. У роботах Чена [3, 7] вперше було представлено схему хамелеон-підпису, вільну від проблеми витоку ключа, без використання GDH груп. Нами обрана саме ця схема для створення хамелеон-підпису на основі ДСТУ 4145-2002, вільного від проблеми витоку ключа.

2. Аналіз властивостей хамелеон-підпису на основі ДСТУ 4145-2002

2.1. Опис схеми хамелеон-підпису на основі ДСТУ 4145-2002

Схема формування хамелеон-підпису (рис.1) на основі ДСТУ 4145-2002 [6] складається з таких етапів:

– обчислення загальних параметрів хамелеон-підпису;

– обчислення одержувачем відкритого та секретного ключів функції геш-хамелеону, після чого відкритий ключ геш-хамелеону передається підписувачу для обчислення функції геш-хамелеону;

– ДСТУ 4145-2002, після чого відкритий ключ підпису передається одержувачу підписаного повідомлення;

– обчислення цифрового передпідпису згідно ДСТУ 4145-2002;

– обчислення базової функції гешування згідно ГОСТ 34.311-95;

– обчислення функції геш-хамелеону;

– формування хамелеон-підпису.

Розглянемо докладніше деякі з вищезазначених етапів.

На етапі «Обчислення загальних параметрів хамелеон-підпису» обирається еліптична крива над полем $E(F_q)$, $|E(F_q)| = n \times cof$, $(P) \subset E(F_q)$, $|(P)| = n$, де n – просте число.

На етапі «Обчислення загальних параметрів функції геш-хамелеону» обирається G – мультиплікативна група з генератором групи g простого порядку q. Визначається криптографічна функція гешування: $H_2 : B \to G^*$, де $B = \{H_1(T) : T \subset \{0,1\}^*\}$, враховуючи, що $H_1 : \{0,1\}^* \to \{0,1\}^r$ – базова функція гешування (згідно ГОСТ 34.311). Загальними параметрами функції геш-хамелеону будуть: $\{G, g, q, H_1, H_2\}$.

На етапі «Обчислення відкритого та секретного ключів функції геш-хамелеону» спочатку виконується алгоритм обчислення секретного ключа функції геш-хамелеону наступним чином: одержувач випадково генерує ціле число $x \in Z_q^*$.

Далі виконується алгоритм обчислення відкритого ключа функції геш-хамелеону наступним чином: відкритий ключ обчислюється як $y = g^x$, його дійсність засвідчується включенням його до складу сертифікату відкритого ключа одержувача.

Етап «Обчислення відкритого та особистого ключів хамелеон-підпису» виконується згідно з ДСТУ 4145-2002 без будь-яких змін. Особистим та відкритим ключем відповідно будуть випадкове ціле d та точка еліптичної кривої виду $Q = -dP$, де P – базова точка еліптичної кривої, а $d \in [1, n-1]$. Далі виконується етап «Обчислення цифрового передпідпису» (згідно з ДСТУ 4145-2002 без будь-яких змін). Цифровий передпідпис позначається як (e, F_r), де e – випадкове число, а $F_r = x_R$ та $R = eP = (x_R, y_R)$.

Вихідні дані алгоритму «Обчислення хамелеон-підпису»:

– загальні параметри хамелеон-підпису;

– особистий ключ хамелеон-підпису d;

– відкритий ключ геш-хамелеону y.

Результат виконання алгоритму: хамелеон-підпис D повідомлення T.

Розглянемо докладніше алгоритм обчислення хамелеон-підпису (відмітимо, що етапи, пов'язані з перевіркою коректності загальних параметрів, оцінкою правильності особистого та відкритого ключів, і таке інше, здійснюються згідно з ДСТУ 4145-2002 без будь-яких змін):

1. Від повідомлення T обчислюється результат базової функції гешування H_1.
2. Обирається випадкове число $a \in Z_q^*$.
3. Обчислюється g^a.
4. Обчислюється $h = H_2(y \| I))$, де $I = ID_S \| ID_R \| ID_T$ – загальний ідентифікатор, ID_S – ідентифікатор підписувача, ID_R – ідентифікатор одержувача, ID_T – ідентифікатор транзакції.
5. За результатом обчислення базової функції гешування H_1 обчислюється значення функції геш-хамелеону $h_{Ch} = H_{Ch}(H_1(T)), g^a, h) = g^a h^{H_1(T)}$, де $H_{Ch} : B \times Z_q^* \times Z_q^* \to Z_q^*$.
6. Результат обчислення функції геш-хамелеону h_{Ch} перетворюється в елемент базового поля $\overline{h}_{Ch}$.
7. Обчислюється передпідпис (e, F_e).
8. Обчислюється елемент базового поля $t = \overline{h}_{Ch} + F_e$.
9. Елемент базового поля t перетворюється на ціле число r.
10. Обчислюється ціле число $s = (e + dr) \bmod n$.
11. Значення хамелеон-підпису визначається як $D = (T, g^a, y^e, r, s)$.

Відмітимо, що етапи 6-10 виконуються згідно з ДСТУ 4145-2002 без будь-яких змін. Запропонований алгоритм хамелеон-підпису на основі ДСТУ 4145-2002 забезпечує властивості, що представлені у табл. 1.

Таблиця 1

Властивість	Опис властивості
Неінтерактивність	Відсутність необхідності зі сторони як підписувача так і одержувача зв'язуватися між собою перед початком формування або перевірки підпису
Неможливість підробки	Неможливість створення валідного ЕЦП будь-ким та одержувачем до генерації його підписувачем
Неспростовність	Неможливість підписувачем у подальшому відмовитись від факту вироблення ЕЦП. Формально це означає, що підписувач не здатен сформувати колізію відносно функції геш-хамелеону
Реверсивність (відновлення повідомлення)	Можливість використання хамелеон-підпису у якості стандартного ЕЦП із додатком (при необхідності). Під стандартним ЕЦП із додатком вважається ЕЦП ДСТУ 4145-2002
Непередаваність ЕЦП	Неможливість доведення одержувачем справжності ЕЦП будь-якій третій стороні без участі підписувача
Прихованість повідомлення	Відсутність необхідності розкриття підписувачем змісту повідомлення будь-якій третій стороні при вирішенні можливих протиріч
Відсутність витоку особистого ключа геш-хамелеону	Неможливість отримання або обчислення підписувачем особистого ключа геш-хамелеону одержувача у разі виникнення протиріччя та, як наслідок, спростування у подальшому повідомлень, що були підписані

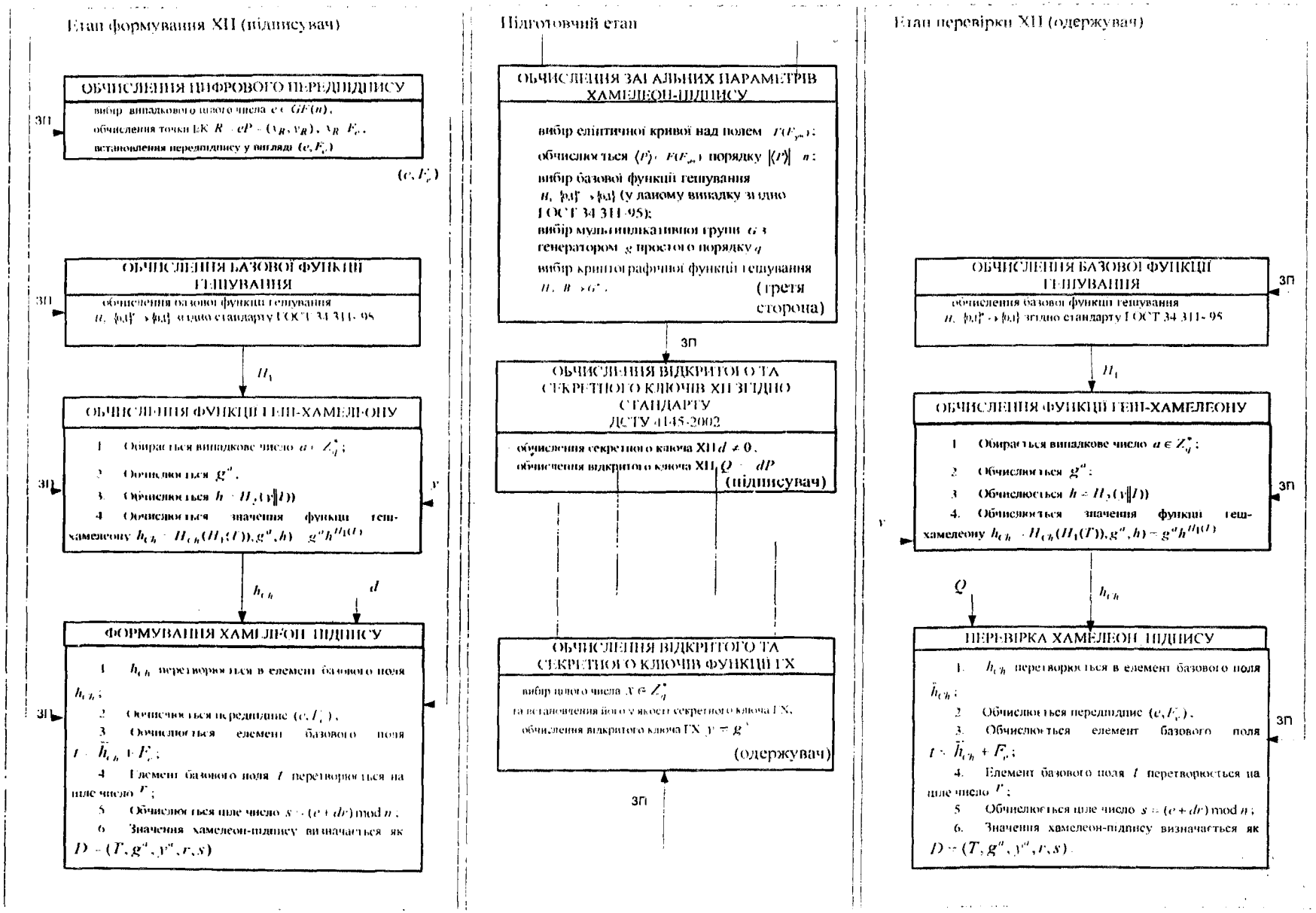
Етап формування ХП (підписувач)
ОБЧИСЛЕННЯ ЦИФРОВОГО ПЕРЕДПИДПИСУ
вибір випадкового цілого числа $e \in GF(n)$,
обчислення точки ЕК $R = eP = (x_R, y_R)$, $x_R \in F_{p^m}$,
встановлення передпидпису у вигляді (e, F_e)
ЗП
(e, F_e)
ОБЧИСЛЕННЯ БАЗОВОЇ ФУНКЦІЇ ГЕШУВАННЯ
обчислення базової функції гешування
$H_1: \{0,1\}^* \to \{0,1\}^l$ згідно стандарту ГОСТ 34.311-95
ЗП
H_1
ОБЧИСЛЕННЯ ФУНКЦІЇ ГЕШ-ХАМЕЛЕОНУ
1 Обирається випадкове число $a \in Z_q^*$;
2 Обчислюється g^a.
3 Обчислюється $h = H_2(y \| I))$
4 Обчислюється значення функції геш-хамелеону $h_{Ch} = H_{Ch}(H_2(I)), g^a, h) = g^a h^{H_2(I)}$
ЗП
y
h_{Ch}
d
ФОРМУВАННЯ ХАМЕЛЕОН-ПІДПИСУ
1 h_{Ch} перетворюється в елемент базового поля $\bar{h}_{Ch}$;
2 Обчислюється передпидпис (e, F_e).
3 Обчислюється елемент базового поля $t = \bar{h}_{Ch} + F_e$;
4 Елемент базового поля t перетворюється на ціле число r;
5 Обчислюється ціле число $s = (e + dr) \bmod n$;
6 Значення хамелеон-підпису визначається як $D = (T, g^a, y^a, r, s)$
ЗП
Підготовчий етап
ОБЧИСЛЕННЯ ЗАГАЛЬНИХ ПАРАМЕТРІВ ХАМЕЛЕОН-ПІДПИСУ
вибір еліптичної кривої над полем $F(F_{p^m})$;
обчислюється $\langle P \rangle \subset F(F_{p^m})$ порядку $|\langle P \rangle| = n$;
вибір базової функції гешування $H_1: \{0,1\}^* \to \{0,1\}^l$ (у лаконому випадку згідно ГОСТ 34.311-95);
вибір мультиплікативної групи G з генератором g простого порядку q
вибір криптографічної функції гешування $H_2: B \to G^*$.
(третя сторона)
ЗП
ОБЧИСЛЕННЯ ВІДКРИТОГО ТА СЕКРЕТНОГО КЛЮЧІВ ХП ЗГІДНО СТАНДАРТУ ДСТУ 4145-2002
обчислення секретного ключа ХП $d \neq 0$,
обчислення відкритого ключа ХП $Q = dP$
(підписувач)
ОБЧИСЛЕННЯ ВІДКРИТОГО ТА СЕКРЕТНОГО КЛЮЧІВ ФУНКЦІЇ ГХ
вибір цілого числа $x \in Z_q^*$
та встановлення його у якості секретного ключа ГХ,
обчислення відкритого ключа ГХ $y = g^x$
(одержувач)
ЗП
Етап перевірки ХП (одержувач)
ОБЧИСЛЕННЯ БАЗОВОЇ ФУНКЦІЇ ГЕШУВАННЯ
обчислення базової функції гешування
$H_1: \{0,1\}^* \to \{0,1\}^l$ згідно стандарту ГОСТ 34.311-95
ЗП
H_1
ОБЧИСЛЕННЯ ФУНКЦІЇ ГЕШ-ХАМЕЛЕОНУ
1 Обирається випадкове число $a \in Z_q^*$;
2 Обчислюється g^a;
3 Обчислюється $h = H_2(y \| I))$
4. Обчислюється значення функції геш-хамелеону $h_{Ch} = H_{Ch}(H_2(I)), g^a, h) = g^a h^{H_2(I)}$
ЗП
y
Q
h_{Ch}
ПЕРЕВІРКА ХАМЕЛЕОН-ПІДПИСУ
1. h_{Ch} перетворюється в елемент базового поля $\bar{h}_{Ch}$;
2 Обчислюється передпидпис (e, F_e).
3. Обчислюється елемент базового поля $t = \bar{h}_{Ch} + F_e$;
4. Елемент базового поля t перетворюється на ціле число r;
5 Обчислюється ціле число $s = (e + dr) \bmod n$;
6. Значення хамелеон-підпису визначається як $D = (T, g^a, y^a, r, s)$.
ЗП

Рис. 1

2.2. Алгоритм взаємодії учасників у разі виникнення протиріч

Розглянемо протокол спростування підробленого підпису. У подальшому під протиріччям розуміється або відмова підписувача від факту формування ЕЦП, або твердження одержувача про факт підписання хибного повідомлення.

У разі виникнення протиріччя одержувач надає третій довіреній стороні (ТДС) підпис $D=(T^*,g^{a*},y^{a*},r,s)$ та неінтерактивне доведення знання Π_1^* рівності двох дискретних логарифмів $x=\log_g y=\log_{g''} y^{a'}$. Якщо D або Π_1^* є недійсними, ТДС відхиляє запит одержувача. Якщо перевірка пройшла успішно, ТДС відправляє підпис підписувачу. Якщо підписувач вважає отриманий підпис дійсним, він підтверджує ТДС цей факт. У протилежному випадку він формує колізію функції геш-хамелеону наступним чином:

1. Якщо підписувач хоче забезпечити властивість «відновлення повідомлення» [7], він надає ТДС набір (T,g^a,y^a,Π_1) у якості колізії, де Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_g g^a=\log_y y^a$. Тільки якщо $T^*\neq T$, $h_{Ch}=g^a h^{H_1(T)}$ та Π_1 є дійним, ТДС може бути впевнена у тому, що одержувач сформував підробку підпису повідомлення T. Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «відновлення повідомлення» представлена на рис. 2.

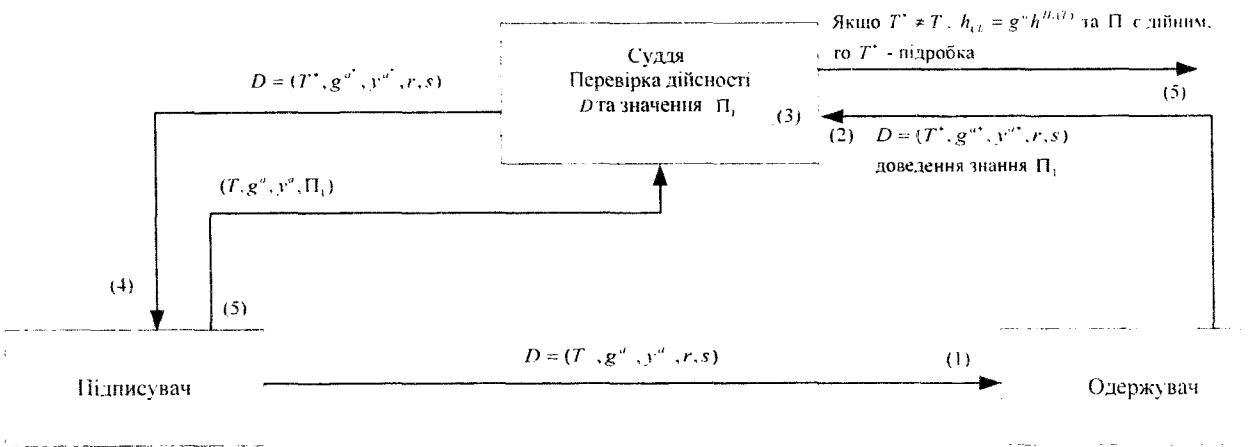

Рис. 2

2. Якщо підписувач хоче забезпечити властивість «прихованість повідомлення» [7], він надає ТДС набір (g^a,y^a,Π_1,Π_2) у якості колізії, де Π_2 – неінтерактивне доведення знання дискретного логарифму $T=\log_h h_{Ch}/g^a$ та Π_1 – неінтерактивне доведення знання рівності двох дискретних логарифмів $\log_g g^a=\log_y y^a$. Тільки якщо, $g^{a*}\neq g^a$, та Π_1,Π_2 є дійсними, ТДС може бути впевненим у тому, що одержувач сформував підробку підпису повідомлення T^*, і водночас, повідомлення T залишилося конфіденційним.

Розгорнутий протокол спростування підробленого підпису у разі необхідності забезпечення властивості «прихованість повідомлення» представлено на рис. 3.

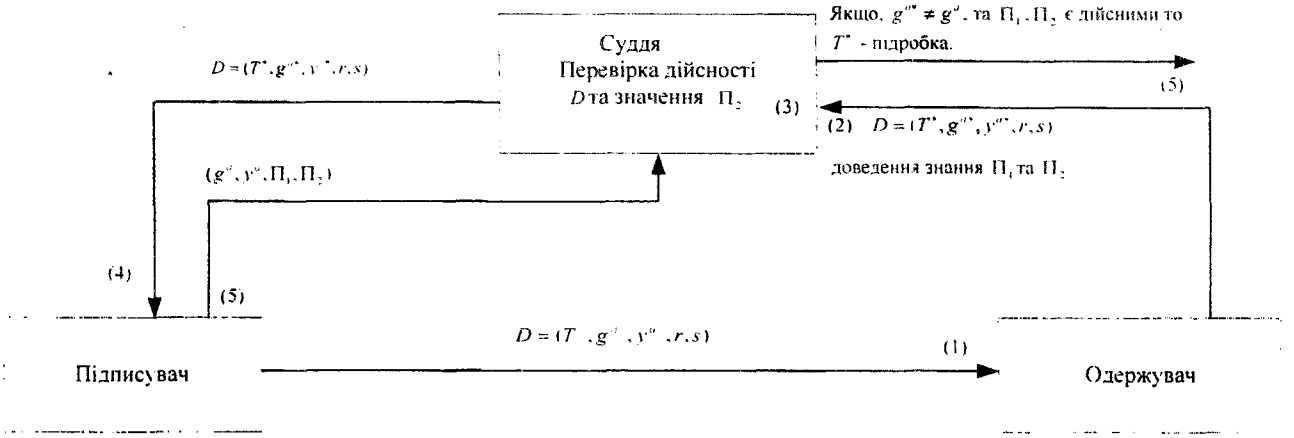

Рис. 3

3. Аналіз складності хамелеон-підпису на основі ДСТУ 4145-2002

Наділення алгоритму ЕЦП додатковими властивостями зазвичай супроводжується зростанням складності обчислень. Тому важливим питанням є вимірювання зростання складності отриманого алгоритму.

У табл. 2 наведено результати порівняльного аналізу складності алгоритму ЕЦП згідно з ДСТУ 4145-2002 та алгоритму хамелеон-підпису на основі ДСТУ 4145-2002. У таблиці використовуються наступні позначення: H – складність обчислення базової функції гешування, M_E – множення на скаляр у групі точок ЕК, M_F – множення у скінченному полі, M_G – множення у скінченній групі, A_E – бінарна операція у групі точок ЕК, E_G – зведення до ступеня у скінченій групі.

Таблиця 2

Процес	ДСТУ 4145-2002	Хамелеон-підпис згідно з ДСТУ 4145-2002
Формування підпису	$1H+1M_E+2M_F$	$2H+1M_E+2M_F+3E_G+1M_G$
Перевірка підпису	$1H+2M_E+1M_F+1A_E$	$2H+2M_E+1M_F+1A_E+2E_G+1M_G$

За результатами табл. 2 відмітимо, що складність хамелеон-підпису відносно складності алгоритму ЕЦП ДСТУ 4145-2002 визначається тільки схемою геш-хамелеону, а саме – наскільки її швидкісні показники відрізняються від базової функції гешування, що використовується у схемі ЕЦП.

У табл. 3 наведено результати порівняльного аналізу складності обчислень геш-хамелеону та геш-функції згідно з ГОСТ 34.311-95. Слід зазначити, що складність алгоритму геш-хамелеону залежить від структури скінченої групи та базової функції гешування. У якості скінченої групи використовується мультиплікативна група поля Галуа, тобто складність функції геш-хамелеону визначатиметься характеристикою поля.

Порівняльний аналіз будемо проводити у залежності від зростання бітової довжини характеристики поля та розміру даних, що будуть гешуватися.

Реалізація алгоритмів гешування виконана мовою програмування Java та тестовий стенд має наступні характеристики: ОС Windows XP SP 3, AMD Athlon 64 X2 Dual Core Processor 3800+ 2.01Ghz, 3.00 Gb of RAM.

Виходячи з отриманих результатів, відмітимо, що при збільшенні характеристики поля та використанні даних розміром до 1 *Кб* швидкість виконання геш-хамелеону уповільнюється відносно базової функції гешування у сотні разів. Але при використанні даних розміром від 1 *Мб* та більше, складність обчислень майже однакова. Це пов'язано з тим, що при обчисленні результату геш-хамелеону спочатку виконується базова функція гешування, а після виконуються 3 операції зведення до ступеня та 1 множення у групі незалежно від об'єму вхі-

дних даних. Таким чином, при зростанні об'єму вхідних даних до базової функції гешування зростання бітової довжини характеристики поля не вноситиме суттєвого вклад у складність обчислення функції геш-хамелеону.

Таблиця 3

	1 *Кб*	1 *Мб*	10 *Мб*
ГОСТ 34-311	0.002 с	2.552 с	25.542 с
Геш-хамелеон – 512	0.006 с	2.592 с	25.657 с
Геш-хамелеон – 1024	0.014 с	2.535 с	25.579 с
Геш-хамелеон – 2048	0.040 с	2.576 с	26.003 с
Геш-хамелеон – 3072	0.084 с	2.618 с	25.434 с
Геш-хамелеон – 4096	0.146 с	2.671 с	25.750 с
Геш-хамелеон – 6144	0.328 с	2.867с	26.682 с
Геш-хамелеон – 8192	0. 571 с	3.090 с	28.010 с

При застосуванні функції геш-хамелеону у протоколах, що передбачають використання даних невеликої довжини (менш ніж 1 *Кб*) зазначимо, що збільшення складності обчислень приблизно у 300 разів є відносним, оскільки таке збільшення є максимальним на довжині характеристики поля у 8192 біта та абсолютний час виконання геш-хамелеону складає приблизно 0,5 *с*.

У табл. 4 наведено приклад обчислення функції геш-хамелеону із бітовою довжиною характеристики поля 512 біт та демонструється формування колізії.

Таблиця 4

Формування функції геш-хамелеону	
Опис	Значення
Рівень стійкості (біт)	512
Характеристика поля	0xEA0D54F24469F1D9C9A850B0AF7346FEF9A09F30BB6 AC6C9966D700849133E0ECF57D4F9F7199842B8D2EDC6F 5823E9644C10A5881343C96B5A41B9BE081F9D3
Генератор групи	0x71C4F7F7BD0F18E8605DADBF0E6674938B4A768D7290 427D7D2793A9CB63FBC968388D7B7059FE6D7A191FA5A A6329B253A6623555BC411CE3FB3D5273521DAE
Порядок групи	0x856E6BA94E3169D3D7EA71764ADF11971703A0F1
Особистий ключ хамелеон-підпису	0x399E744F7E09EAC152B161989616A2C7D4EE6DB4
Відкритий ключ геш-хамелеону	0xE5099FE4EE5AEFBC40C6CE5047ED9943083BB0427D46 FB0D9A45CEBE5606A482032C83DA9E0035CE36D60186E 67F8150A1F29440FA4F09FD72D63927749F0FB3
Ідентифікатор підписувача	Підписувач
Ідентифікатор одержувача	Одержувач
Ідентифікатор транзакції	1324564
Повідомлення T	abcdefghij
Значення функції геш-хамелеону	0x3505A80A448902937CE404CF226E349B99B6E02FBF0E6 84198303C61CE498713
Формування колізії	
Повідомлення T^*	123456789
Значення функції геш-хамелеону	0x3505A80A448902937CE404CF226E349B99B6E02FBF0E6 84198303C61CE498713

Висновки

Сучасні вимоги бізнесу у сфері електронної комерції потребують забезпечення додаткових послуг безпеки. Аналіз доступних джерел дозволяє зробити висновок, що забезпечення цих властивостей потребує застосування нових концепцій та вдосконалення існуючих меха-

нізмів захисту інформації, проте вдосконалення існуючих схем не повинно призводити до суттєвого погіршення характеристик (наприклад, складність обчислень, стійкість, пропускна здатність тощо), що ними забезпечувались. У роботі викладаються результати досліджень, що дозволяють запропонувати нове застосування національного стандарту ЕЦП ДСТУ 4145-2002 у сферах закритих інтернет-аукціонів та системах закритого електронного голосування [8,9]. Таке вдосконалення стало можливим за рахунок інтеграції до ЕЦП ДСТУ 4145-2002 геш-функції спеціального виду (геш-хамелеон). Запропонована схема забезпечує ряд властивостей, серед яких основними є непередаваність ЕЦП та прихованість повідомлення. Наділення базової схеми ЕЦП новими властивостями не зменшує її рівень стійкості, що визначається специфікою інтеграції функції геш-хамелеону у зазначену схему ЕЦП.

На основі теоретичних досліджень схеми хамелеон-підпису було отримано аналітичний вираз для складності обчислень. Збіг теоретично очікуваних результатів та результатів практичної реалізації доводять їх достовірність. Аналіз часової складності схеми хамелеон-підпису проводився без врахування протоколів спростування підробленого підпису як і з забезпеченням властивості «відновлення повідомлення», так і властивості «прихованість повідомлення», оскільки вони виконуються лише у випадку виникнення протиріччя.

Відмітимо, що запропонована схема хамелеон-підпису у порівнянні за схемою ДСТУ 4145-2002 має близькі за значенням швидкісні характеристики. Відхилення від показників швидкодії при зростанні рівня стійкості геш-хамелеону спостерігається лише на малих довжинах повідомлень, але таке відхилення є відносним та не заважає його практичному застосуванню, зокрема у системах закритих інтернет-аукціонів та закритого електронного голосування.

У межах подальших досліджень планується створення функції геш-хамелеону в групі точок ЕК з метою вдосконалення схеми хамелеон-підпису на основі ДСТУ 4145-2002 на етапі генерування загальносистемних параметрів, а також детальний аналіз стійкості запланованої схеми.

Список літератури: 1. *H. Krawczyk and T. Rabin*, Chameleon hashing and signatures Proc. of NDSS. – 2000. – P.143-154, 2000. 2.*G. Ateniese and B. de Medeiros*. Identity-based chameleon hash and applications. FC 2004, LNCS 3110, Springer-Verlag, 2004, pp.164-180. 2. X. Chen, F. Zhang, and K. Kim, Chameleon hashing without key exposure, ISC 2004, LNCS 3225, Springer-Verlag, 2004, pp.87-98. 3. *G. Ateniese and B. de Medeiros*. On the key exposure problem in chameleon hashes. SCN 2004, LNCS 3352, Springer-Verlag, 2005, pp.165-179. 4. *W. Gao, F. Li, and X. Wang*, Chameleon hash without key exposure based on Schnorr signature, Computer Standards and Interfaces 31, 2009, pp. 282-285. 5. *ДСТУ 4145-2002* "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння". 6. *X. Chen, F. Zhang*, Key-Exposure Free Chameleon Hashing and Signatures Based on Discrete Logarithm Systems, Cryptology ePrint Archive: Report 2009/035, 2009. 7. *А.В. Лєншин, Ю.М. Іщенко*, Додаткові властивості безпеки електронних транзакцій у системах, що використовують сервіси комбінованої ІВК // Вісник Харк. нац. ун-ту ім. В.Н. Каразіна. – №890. Сер. Математичне моделювання. Інформаційні технології. Автоматизовані системи управління". – Х., 2010. – Вип. 13. – С. 109-114. 8. *Ю.М. Лєншина, Д.С. Беляк*, Реалізація послуги приватності у схемі інтернет-аукціону з використанням хамелеон-підпису // Системи обробки інформації. Інформаційні технології та комп'ютерна інженерія. – Х., 2011. – Вип. 3(93). – С. 126-129.

Харківський національний університет радіоелектроніки

Надійшла до редколегії 15.08.2011