АССИМЕТРИЧЕСКИЕ КРИПТОГРАФИЧЕСКИЕ ПРЕОБРАЗОВАНИЯ

УДК 681.3.06

СХЕМА ЦИФРОВОГО ПІДПИСУ ІЗ ВИКОРИСТАННЯМ ПАРНИХ ВІДОБРАЖЕНЬ НА ОСНОВІ СТАНДАРТУ ДСТУ4145-2002

І.Д. ГОРБЕНКО, К.А. ПОГРЕБНЯК

В роботі пропонується схема цифрового підпису на основі стандарту ДСТУ4145-2002 із використанням парних відображень типу Вейля та Тейта. Досліджуються питання доведення стійкості та складності криптоперетворень у зазначеному цифровому підписі.

The paper presents an identity-based signature scheme based on DSTU4145-2002 standard with use of Weil or Tate bilinear pairings. Problems of proving the strength and complexity of cryptotransformations involved in the mentioned digital signature are studied.

1. АКТУАЛЬНІСТЬ ВПРОВАДЖЕННЯ СХЕМИ ЕЦП ІЗ ВИКОРИСТАННЯМ ПАРНИХ ВІДОБРАЖЕНЬ В УКРАЇНІ

Високі темпи інвестування інфраструктури відкритих ключів (ІВК) прогнозують спеціалісти компанії Datamonitor. У своєму звіті «Creating Trust: PKI and authentication and encryption technologies» вони стверджують, що програмні системи на основі ІВК у найближчий час стануть основним вибором у галузі електронного бізнесу для надання послуг автентифікації, неспростовності, конфіденційності та інших [1]. Темпи зростання популярності ІВК ще більш поширяться з розвитком бездротових комунікацій, а оператори бездротового зв'язку стануть одними з важливіших користувачів цієї технології, а також основним каналом розповсюдження цифрових сертифікатів.

На наш погляд поширення ІВК відбувається з двох причин.

По-перше, постійне зростання швидкісних властивостей мікропроцесорів підвищили доступність електронного цифрового підпису (ЕЦП) користувачам мобільних пристроїв та ЕОМ.

По-друге, зростаюча складність та широке розповсюдження комунікаційних систем створили необхідність в потужних механізмах контролю доступу. Саме технологія цифрових сертифікатів здатна забезпечити оптимальні рішення з управління доступом та безпечність електронного документообігу.

В Україні, з урахуванням досвіду технологічно розвинених держав, створено інформаційну структуру підтримки електронного цифрового підпису, введено у дію Центральний засвідчувальний орган, уже здійснено акредитацію та офіційно функціонують ряд центрів сертифікації ключів [2, 3]. Але практичний досвід виявив ряд недоліків, серед яких, на нашу думку, найбільш вагомими є наступні:

1. Для впровадження системи на базі ІВК необхідно вирішити багато юридичних питань, що зазвичай вимагає значного часу. Більш того, існують проблеми, що стосуються нормативно-правового забезпечення для створення повнофункціональної ІВК. Так, на нинішній час не завершено гармонізацію міжнародних стандартів, що стосуються методів, механізмів, протоколів та основних положень відносно криптографічного захисту повнофункціональних систем електронного документообігу. В недостатній мірі вирішені питання стандартизації форматів та специфікації даних.

2. Необхідність існування єдиного стандарту на цифрові сертифікати, який дозволяє створити функціональну сумісність програмних та апаратних засобів підтримки ІВК. Параметри сертифікатів повинні однозначно тлумачитись незалежно від виробника додатків, які користуються послугами ІВК. Для України ця проблема особливо актуальна, оскільки навіть сертифіковані системами криптографічного захисту інформації (КСЗІ) різних виробників можуть бути не сумісні.

3. Повноцінне функціонування ІВК не може бути здійснене без участі держави. Активне використання технології ІВК потребує більшої гнучкості правового регулювання в області застосування засобів ЕЦП. Тому доцільно створити багаторівневий підхід до визнання юридичної сили ЕЦП, ліцензування та розмежування вимог для адміністративної сфери, корпоративної, документообігу тощо.

4. Для впровадження в дію системи на базі ІВК необхідно витратити досить великі кошти, що пов'язано зі складністю всієї інфраструктури. Сюди входить проектування та розробка всіх елементів системи, навчання обслуговуючого персоналу, витрати на технічне забезпечення. У подальшому необхідно витрачати великі кошти на утримання приміщення, заробітну платню обслуговуючому персоналу, фізичний захист приміщення, переатестацію тощо. Ураховуючи це,

необхідно залучати значні інвестиції на створення та підтримку ІВК, що не завжди є комерційно вигідним.

5. Кожна система захисту повинна бути зручною для користувачів. Сутність зручності полягає у прозорості такої системи для користувачів системи захисту. На жаль, така проблема для користувачів ІВК існує і на нинішній день. Дуже важко створити систему, яка була б прозора для кінцевих споживачів і не потребувала додаткових знань для її використання.

6. Перш ніж випустити сертифікат, засвідчувальний орган повинен ідентифікувати заявника. Це потребує нового підходу та використання певних часових ресурсів, оскільки у разі пред'явлення несправжніх документів засвідчувальний орган може понести значні збитки та втратити репутацію.

7. Діюча ІВК має постійно накопичувати відкликані та скасовані сертифікати, оновлювати списки відкликаних сертифікатів, перевіряти отримані сертифікати на валідність, що потребує певних витрат, які постійно зростають.

Необхідність спрощення ІВК призвела до появи альтернативної архітектури, в основу якої покладено використання ідентифікаторів (identity-based cryptography). Проте, альтернативні системи не в змозі повністю замінити діючу ІВК, так як разом з перевагами вони також містять і певні недоліки [4]. Порівняльний аналіз систем ІВК з використанням сертифікатів та систем на базі ідентифікаторів наведено у табл. 1.

Ураховуючи недоліки та переваги зазначених систем, вирішення протиріч полягає у використанні комбінованої архітектури [6].

Зважаючи на активні пошуки удосконалення та спрощення ІВК у розвинутих країнах світу, а також дослідження альтернативного напрямку використання криптографії на базі ідентифікаторів та можливості її інтеграції у ІВК, постає проблема впровадження систем із використанням ідентифікаторів в діючу ІВК України. Виникає також необхідність у дослідженні таких систем та прогнозуванні їх подальшого розвитку, що дозволить виділити особливості використання їх у національному електронному документообігу.

Відомо, що використання криптографії на базі ідентифікаторів дозволяє вирішити ряд протиріч та проблемних питань у частині електронних цифрових підписів та направленого шифрування. Для використання комбінованих систем ІВК в Україні треба пристосувати існуючі протоколи із використанням ідентифікаторів до діючих національних стандартів [7-9]. Зважаючи на те, що національна ІВК в основному зорієнтована на надання послуг ЕЦП, першочерговою задачею є створення аналогу національної схеми цифрового підпису, який буде базуватися на використанні ідентифікаційних даних. Така модель дозволить зробити перший крок на шляху впровадження національної комбінованої системи та у подальшому може спростити процедуру стандартизації та нормативно-правового забезпечення комбінованої архітектури.

Таблиця 1

Порівняння архітектури на базі ідентифікаторів та традиційної ІВК

№	Критерій порівняння	Системи на ідентифікаторах	Традиційна ІВК
1	Об'єкти довіри	Повна довіра до УГ, який виробляє закритий ключ	Часткова довіра до ЦС
2	Автентичність ключів	За рахунок ідентифікатора	Використання сертифікатів
3	Генерування ключів	УГ генерує закритий ключ, а користувач – відкритий	Користувач генерує пару відкритий – закритий ключ
4	Питання відкликання	Відкликання за рахунок додавання позначки часу до ідентифікатору	Підтримка OCSP та CBC
5	Розповсюдження ключів	Не потрібне	Потрібне
6	Належність користувача до системи	Не потрібна реєстрація	Необхідність отримання сертифікатів, CBC та попередня реєстрація
7	Зберігання закритих ключів	Отримуються повсякчас, зберігаються не довго	Необхідно зберігати досить довго
8	Підтримка відкритих ключів	Не має необхідності	Підтримка каталогів сертифікатів, CBC
9	Відтворення ключів	Можливе	Неможливе
10	Вартість системи	Втричі дешевше [5]	Досить дорога
11	Навантаження на систему	В три рази менша активність [5]	Висока активність користувачів в системі
12	Складність архітектури	Менш складна	Складна
13	Прозорість для користувача	Прозора	Потрібна підготовка
14	Нормативно правова база	Не розвинута	Розвинута
15	Наявність закритого каналу зв'язку	Потрібен автентичний канал	Попередня реєстрація

2. СХЕМА ЕЦП З ВИКОРИСТАННЯМ БІЛІНІЙНИХ ВІДОБРАЖЕНЬ НА ОСНОВІ СТАНДАРТУ ДСТУ4145-2002

На сьогоднішній час створення ефективного цифрового підпису, який використовує концепцію ідентифікаторів, потребує застосування білінійних відображень типу Вейля або Тейта. Математичний апарат та огляд спарювань буде використано відповідно до [10,11]. Основу цифрового підпису буде складати національний стандарт ДСТУ4145-2002 [7] та схема цифрового підпису Патерсона [12].

Для побудови удосконаленої моделі цифрового підпису необхідно визначитись із використанням генератору випадкових послідовностей, який призначений для отримування випадкових даних, що застосовуються при побудові загальних параметрів цифрового підпису, обчислення цифрового підпису, а також для побудови відкритих і особистих ключів цифрового підпису. Зважаючи на рекомендацію стандарту ДСТУ4145-2002, будемо використовувати генератор псевдовипадкових послідовностей, визначений у додатку А вказаного стандарту.

Використаємо симетричне спарювання Тейта. Вважатимемо, що задані:

– G_1 – адитивна група точок еліптичної кривої простого порядку n над розширеним полем характеристики два;

– G_2 – підгрупа мультиплікативної групи скінченого поля з порядком, як у групи G_1;

– e – парне відображення Тейта;

– Геш-функція $H_1 : \{0,1\}^* \to G_1$, що відображує ідентифікатор користувача у точку на еліптичній кривій;

– Геш-функція $H_2 : \{0,1\}^* \to F_{2^m}$, що відображує повідомлення користувача у елемент скінченого поля;

– Геш-функція $H_3 : G_2 \to F_{2^m}$.

Формально схема цифрового підпису матиме чотири етапи: ініціалізація, генерування пари особистий – відкритий ключі, підписування, перевіряння.

На етапі ініціалізації центр генерування ключів (ЦГК) виробляє пару відкритий-закритий майстер-ключ центру, тобто генерує випадкове число s та обчислює $P_{pub} = sP$.

Нехай ID – ідентифікатор підписувача, тоді генерація відкритого та особистого ключа користувача виконується наступним чином:

$$\begin{aligned} Q_{ID} &= H_1(ID) \\ d_{ID} &= -sQ_{ID}, \end{aligned} \tag{1}$$

де d_{ID} – особистий ключ користувача, Q_{ID} – відкритий ключ користувача, s – особистий майстер-ключ ЦГК.

При формуванні ЕЦП використовується цифровий передпідпис. Для отримання цифрового передпідпису генерується ціле число l, таке що $0 < l < n$. Далі обчислюється:

$$\begin{aligned} Q &= lP \\ R &= e(P,Q). \end{aligned} \tag{2}$$

Цифровим передпідписом є значення

$$F_l = H_3(R).$$

Процедура формування цифрового підпису полягає у обчисленні значення:

$$S = Q + H_2(M)H_3(R)d_{ID}. \tag{3}$$

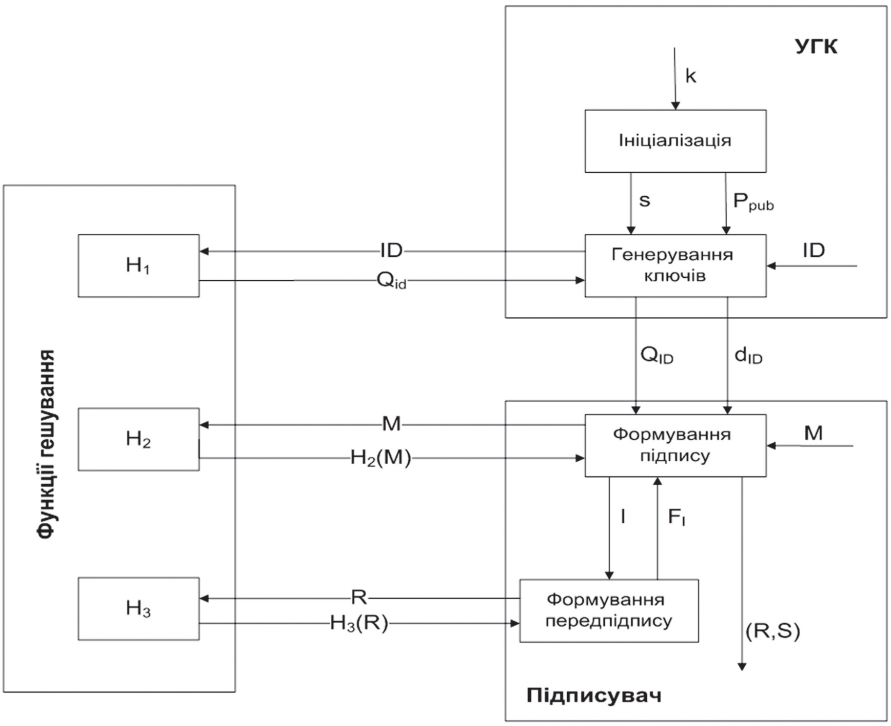

Рис. 1. Схема формування ЕЦП на основі ДСТУ4145-2002 з використанням парних відображень

Сукупність елементів (R,S) являє собою цифровий підпис.

Формально схема вироблення цифрового підпису зображена на рис. 1.

Опишемо процедуру перевірки. Припустимо, що суб'єкт перевірки має повідомлення із ЕЦП, відкритий ключ підписувача та відкритий майстер-ключ УГ. Тоді двійкове подання цифрового підпису представляється у вигляді двох елементів (R,S) згідно формату ЕЦП.

У подальшому обчислюється:

$$R' = e(P,S)e(P_{pub}, H_2(R)H_3(R)Q_{ID}) . \qquad (4)$$

Якщо $R = R'$, тоді підпис визнається дійсним, інакше – підпис недійсний.

Формально схема перевіряння цифрового підпису зображена на рис. 2.

Доведемо правильність алгоритму перевіряння цифрового підпису.

Твердження 1. *Алгоритм обчислення цифрового підпису згідно схем, які зображено на рис. 1 та 2, коректний та задовольняє вимогам, які пред'являються до ЕЦП із додатком.*

Для доведення твердження вважатимемо, що використовуються стійкі до колізій функції гешування. Основне криптографічне перетворення при обчисленні цифрового підпису виконується над елементом $H_2(M)$ основного поля. Якщо отримане повідомлення ідентичне оригінальному, то під час перевіряння підпису буде обчислено точно той самий елемент основного поля. Якщо цифровий підпис прийнято без спотворень, то для перевіряння цифрового підпису буде використана та сама пара (R,S), яка була отримана під час обчислення цифрового підпису. Під час перевіряння обчислюють число R, а саме

$$R = e(P,S)e(P_{pub}, H_2(M)H_3(R)Q_{ID}) =$$
$$= e(P,S)e(sP, H_2(M)H_3(R)Q_{ID}) =$$
$$e(P,S)e(P, -H_2(M)H_3(R)d_{ID}) =$$
$$= e(P, H_2(M)H_3(R)d_{ID})e(P,Q)\times$$
$$\times e(P, -H_2(M)H_3(R)d_{ID}) = e(P,Q).$$

Тобто, процедури перевіряння та підписування є зворотними, що і доводить твердження. □

Зазначимо, що викривлення повідомлення або будь-яких даних двійкового подання цифрового підпису, що передається, призведе до помилки у перевірці.

3. АНАЛІЗ СКЛАДНОСТІ УДОСКОНАЛЕНОЇ СХЕМИ ЕЦП

Визначимо обчислювальну складність алгоритмів формування та перевіряння ЕЦП, що наведено у схемах на рис. 1 та 2. Алгоритм формування потребує обчислення двох геш-значень,

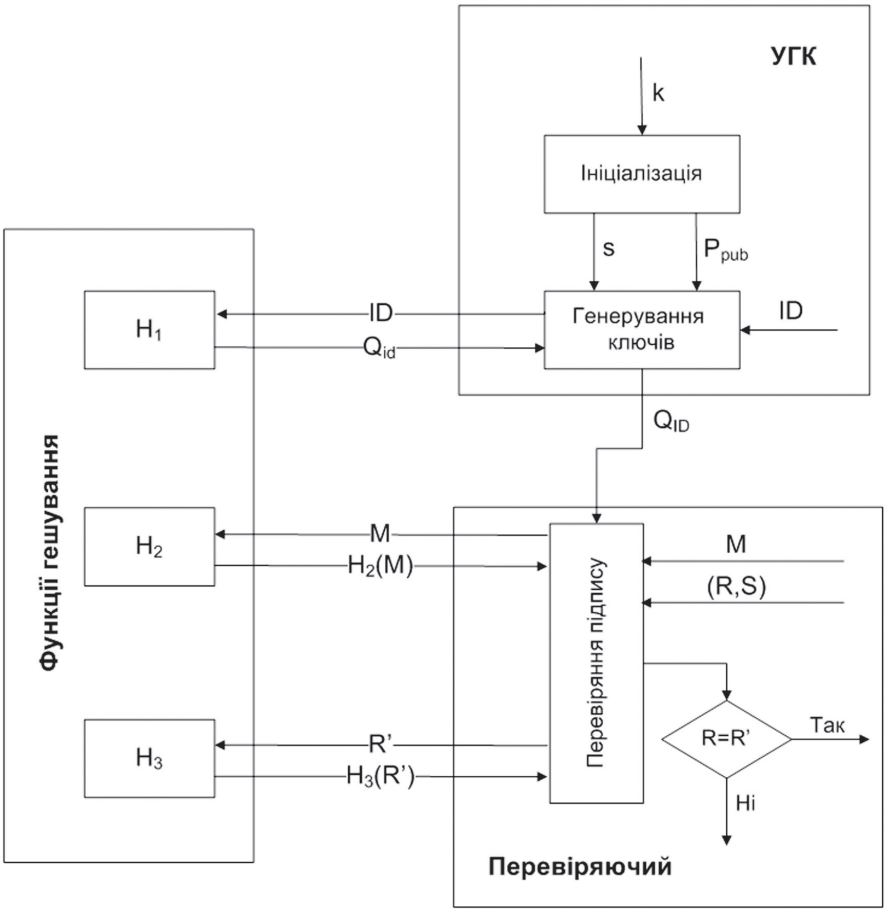

Рис. 2. Схема перевіряння ЕЦП на основі ДСТУ4145-2002 з використанням парних відображень

одного парного відображення, одного множення у розширеному полі характеристики два, двох множень точки еліптичної кривої на скаляр та одного складання у групі G_1. Тобто, отримаємо формулу складності обчислення цифрового підпису:

$$\Sigma_{\text{підп}} = 1M_F + 2H + 1P + 2M_E + 1A_E, \qquad (5)$$

де M_F – операція множення у полі F_{2^m}; H – операція отримання геш-значення; P – функція обчислення парного відображення; M_E – множення на скаляр у групі точок еліптичної кривої $E(F_{2^m})$; A_E – операція додавання у групі G_1.

Алгоритм перевірки потребує двох обчислень геш-значень, двох спарювань, одного множення в полі F_{2^m} та одного експоненціювання у скінченому полі, тобто має складність:

$$\Sigma_{\text{перевір}} = 1M_F + 2H + 2P + 1E_F, \qquad (6)$$

де M_F – операція множення у полі F_{2^m}; H – операція отримання геш-значення; P – функція обчислення парного відображення; E_F – експоненціювання у групі G_2.

Зважаючи на формули (5) та (6), практичну цікавість має порівняння ЕЦП згідно стандарту ДСТУ4145-2002 та аналога такого ЕЦП з використанням білінійних відображень, яке наведено у табл. 2.

Зауважимо, що A_E – це операція додавання у групі точок еліптичної кривої, а A_F – операція додавання у скінченому полі.

Згідно табл. 2 ЕЦП з використанням білінійних відображень на основі ДСТУ4145-2002 вимагає виконання більше операцій, тобто має більшу складність крипто перетворень. Але враховуючи те, що функції гешування мають невеликий вплив на оцінку складності крипто перетворень в порівнянні з операціями у групі точок еліптичної кривої, можливість попереднього обчислення спарювання точок при обчисленні цифрового передпідпису, а також відсутність множення на скаляр у процедурі перевіряння, можливо зробити висновок, що ЕЦП з використанням білінійних відображень на основі ДСТУ4145-2002 наближена до часових характеристик національної схеми ЕЦП.

4. АНАЛІЗ СТІЙКОСТІ УДОСКОНАЛЕНОЇ СХЕМИ ЕЦП

При первинному аналізі зрозуміло, що стійкість схеми ЕЦП залежить від білінійної задачі Діффі-Геллмана. Припускається, що зловмиснику відомі наступні значення: e, kP, Q_{ID}, P_{pub}. Оскільки група G_1 циклічна, то $Q_{ID} = dP$. Таким чином, криптоаналітик повинен знайти $e(P,P)^{kds}$.

Існують два погляди світової спільноти фахівців, щодо складності білінійної проблеми Діффі – Геллмана. Деякі вчені вважають, що не пройшло достатньо часу на розвиток математичного апарату, який би довів або спростував твердження, щодо складності зазначеної проблеми. Але більшість вважають, що білінійна проблема Діффі – Геллмана є стійкою. Аналіз відносин класичних проблем Діффі –Геллмана та їх білінійних аналогів, а також наш погляд стосовно їх класифікації відображені в роботі [13].

Для доведення стійкості схеми цифрового підпису, зазвичай достатньо довести стійкість проти екзистенційної підробки на основі атаки з вибором підписаних повідомлень. Тобто, криптоаналітик може вибирати відкритий ключ та підписане повідомлення. При цьому вибір наступного підписаного повідомлення він може робити на основі знання підпису попереднього обраного повідомлення. Мета, яку прагне досягти криптоаналітик, полягає у створенні будь-якого повідомлення, що має такий самий підпис, як і перехоплене.

Для доказу стійкості цифрового підпису до екзистенційної атаки із адаптивним вибором підписаного повідомлення, зазвичай використовується модель, що описана в роботі [12]. Якщо зробити припущення, що функції гешування, які передбачаються цифровим підписом, є криптографічно стійкі, то модель доведення є майже такою, як в зазначеній роботі.

ВИСНОВКИ

В роботі запропоновано схему цифрового підпису із використанням парних відображень на основі стандарту ДСТУ4145-2002. Така конструкція цифрового підпису дає змогу змоделювати комбіновану національну систему документообігу, яка вміщуватиме в собі переваги як діючої ІВК, так і архітектури на основі ідентифікаторів.

У подальшому, для реалізації зазначеної комбінованої архітектури, застосування схеми цифрового підпису, що пропонується на базі національного стандарту, дасть можливість скоротити витрати на розробку нормативно-правової бази.

Для більш глибокого вивчення умов застосування ЕЦП необхідно вирішити задачі генерування загальносистемних параметрів. Такі параметри мають відповідати додатку Г стандарту [7]. Таким чином, першочерговою задачею є вивчення ме-

Таблиця 2

Порівняльний аналіз складності крипто перетворень у ЕЦП

Схема ЕЦП	Підписування	Перевіряння
ЕЦП з використанням білінійних відображень на основі ДСТУ4145-2002	$1M_F + 2H + 1P + 2M_E + 1A_E$	$1M_F + 2H + 2P + 1E_F$
ЕЦП згідно ДСТУ4145-2002	$2M_F + 1H + 2M_E + 1A_F$	$2M_E + 1M_F + 1H + 1A_F$

тодів побудови загальносистемних параметрів для схеми цифрового підпису з використанням парних відображень для скінчених полів характеристики два.

Враховуючи порівняльний аналіз схеми ЕЦП згідно ДСТУ4145-2002 та її аналога на основі спарювань по критерію швидкодії криптоперетворень, слід зазначити, що схема ЕЦП, яка пропонується, має більшу складність. Але, беручи до уваги переваги криптографічних примітивів з використанням спарювань та постійний процес вдосконалення швидкісних характеристик функції спарювання, можливо стверджувати про конкурентоспроможність схеми ЕЦП, яка наведена у роботі.

Як було визначено, аналіз стійкості ЕЦП, що пропонується, задовольняє сучасним вимогам, які пред'являються до ЕЦП з використанням парних відображень типу Вейля або Тейта. Але у подальшому слід визначити більш детально схеми гешування, які використовуються, та зробити більш детальний аналіз стійкості відповідно до обраних функцій гешування.

На наш погляд, в Україні слід використовувати для побудови криптографічно стійких функцій гешування стандарт ГОСТ34.311 [14]. Головне, щоб функція гешування була стійкою до колізій.

З практичної точки зору цікавим є побудування макету комбінованої архітектури з використанням ЕЦП на основі білінійних відображень та інтеграцію такого макету у національну систему документообігу України. Такий макет дозволить визначити особливості впровадження комбінованої архітектури в Україні та допоможе виявити недоліки схеми ЕЦП, якщо такі маються.

Література.

[1] Creating trust – PKI and authentication and encryption technologies: Datamonitor Report, 2001.

[2] Д. Мялковский, А. Скиба. Организационно-технические вопросы построения и функционирования национальной системы ЭЦП // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні – № 6, 2003. – С. 11–15.

[3] *І.Д. Горбенко, В.А. Демехін, Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, С.С. Батюшко.* Стан та проблемні питання створення та розвитку національної інфраструктури відкритих ключів. // Прикладна радіоелектроніка. – Том 5. 2006. – № 1. – С. 41–51.

[4] Voltage Security. Identity-Based Encryption and PKI Making Security Work. 2005.

[5] The Total Cost of Ownership for Voltage Identity-Based Encryption Solutions. Ferris Research Report, 2006.

[6] *J. Callas.* Identity-Based Encryption with Conventional Public-Key Infrastructure. // In 4th Annual PKI R&D Workshop – № 7224 in Interagency Reports, NIST, 2005. – pp. 102–115.

[7] ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. – К. Держстандарт України, 2003. – 94 с.

[8] Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003р.

[9] Закон України «Про електронний цифровий підпис» від 22 травня 2003 р.

[10] *Горбенко И.Д., Мелецкий А.П., Погребняк К.А., Шевченко Д.В.* Билинейные спаривания эллиптических кривых и его теоретические основы. Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Том 5, 2006, №1.

[11] *Горбенко И.Д., Мелецкий А.П., Погребняк К.А., Шевченко Д.В.* Методы выполнения билинейных спариваний точек эллиптических кривых в криптографических приложениях. Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Том 5, 2006, №1

[12] *Kenneth G. Paterson*. ID-based signatures from pairings on elliptic curves. // IEEE Communications Letters, 38(18):1025–1026, 2002.

[13] *Горбенко І.Д. Погребняк К.А.* Класи складностей в асиметричній криптографії // Міжнародний симпозіум «Питання оптимізації обчислень (ПОО-XX-XIII)»: Праці міжнародного симпозіуму. – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України, – 2007. – С. 80.

[14] ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хеширования. – Москва. Госстандарт России, 1994.

Надійшла до редколегії 4.09.2009

Горбенко Іван Дмитрович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій ХНУРЕ, головний конструктор ЗАТ «Інститут інформаційних технологій». Область наукових інтересів: криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Погребняк Костянтин Анатолійович, аспірант каф. БІТ ХНУРЕ, математик ЗАТ «ІІТ». Область наукових інтересів: застосування алгебраїчної геометрії у системах криптографічного захисту інформації, асиметрична криптографія.