УДК 681.3

Ю.В. Морозов
Національний університет ”Львівська політехніка”,
кафедра “Електронні обчислювальні машини”

ІНТЕЛЕКТУАЛЬНА КАРТА ДЛЯ СИСТЕМИ ЦИФРОВОГО ПІДПИСУ

Розглядається варіант інтелектуальної карти для використання у системі цифрового підпису на основі інфраструктури відкритих ключів.

In the report is considered the variant of construction of smart card for the digital signature system.

1. Вступ

На сучасному етапі розвитку людства інформація вважається основним ресурсом розвитку цивілізації. Електронна інформація з кожним роком визначає дії не тільки все більшої кількості людей, але й все більшого числа технічних систем, створених людиною. Отже, стає зрозуміло, що порушення безпеки обробки й передачі електронної інформації призводить до втрат, ступінь і масштаби яких визначаються цільовим призначенням цієї інформації і можуть бути співмірні з глобальними трагічними випадками.

В Україні широко впроваджуються інформаційні технології практично у всі галузі економіки. Все більша кількість організацій переходить на електронний документообмін. А отже, необхідні власні розробки в напрямку розробки та стандартизації засобів захисту інформації, які відповідають міжнародним нормам і забезпечують потреби нашої країни.

Загальноприйнятим методом захисту електронного документообміну є системи формування цифрового підпису, які забезпечують достовірність отриманої інформації та однозначно ідентифікують відправника.

Сьогодні в Україні для криптографічного закриття інформації та формування цифрового підпису використовуються адаптовані відповідні стандарти СРСР та РФ (ГОСТ28147–89 та ГОСТ Р 34.10–94). Це робить Україну деякою мірою залежною від РФ. У 2001 році в РФ був прийнятий новий стандарт цифрового підпису. Отже, зараз Україні потрібна система для забезпечення інфраструктури цифрових підписів у масштабах країни, якій можна було би надати статус національного стандарту.

Нагадаємо, що основними компонентами для формування цифрового підпису є одностороння хеш-функція та криптосистема з відкритими ключами.

Хеш-функція призначена для формування цифрового дайджесту документа. Даний дайджест потрібний для однозначної ідентифікації документа. Від якості алгоритму хеш-функції залежить стійкість ідентифікації. Для реалізації односторонньої хеш-функції можна використовувати або симетричну криптографічну систему, або спеціально розроблену для цього функцію. Найбільш широковживаними є алгоритми SHA–1 та MD5. Але вони вже не забезпечують необхідної в найближчому майбутньому криптографічної стійкості, тому зараз розробляється алгоритм SHA–2.

Алгоритми відкритих ключів потрібні для однозначної ідентифікації автора документа. Більшість алгоритмів з відкритими ключами базуються на таких принципах:

1. Рюкзак – є множина унікальних чисел, потрібно знайти підмножину, сума яких дорівнює N;

2. Дискретний логарифм – якщо p – просте число, а g та M – цілі числа, потрібно знайти x, для якого виконується

$$g^x \equiv M \pmod{p}$$

3. Розклад на множники – якщо N – добуток двох простих чисел, то потрібно:

- Розкласти N на множники;
- Для заданих цілих чисел M та C знайти d, для якого

$$M^d \equiv C \pmod{N}$$

- Для заданих цілих чисел e та C знайти M, для якого

$$M^e \equiv C \pmod{N}$$

- Для заданого цілого числа x визначити, чи існує ціле число y, для якого

$$x \equiv y^2 \pmod{N}$$

Розглянемо коротко існуючі стандарти цифрового підпису на прикладі стандартів США FIPS PUB 186-2 (DSS) як відкритого та достатньо дослідженого та діючого зараз на Україні стандарту ГОСТ Р 34.10-94.

DSS передбачає використання як хеш-функції функцію, визначену стандартом SHS (алгоритм SHA-1 FIPS PUB 180-1). Для реалізації криптосистеми з відкритими ключами в американському стандарті передбачено три варіанти:

- Перший варіант – використання алгоритму цифрового підпису DSA, що є варіантом алгоритмів цифрового підпису Schnorr та ElGamal. Цей алгоритм базується на проблемі обчислення дискретних логарифмів у скінченному полі. Стандарт передбачає використання ключів довжиною від 512 до 1024 біти. При довжині ключа 1024 біта цей алгоритм забезпечує достатній рівень захисту. Він дещо повільніший за RSA при перевірці цифрового підпису, але при теперішньому рівні обчислювальних потужностей це практично непомітно.
- Другим варіантом є використання алгоритму RSA. Його стійкість заснована на проблемі розкладання на множники великих чисел. Хоча цей алгоритм дуже поширений і підтриманий багатьма світовими організаціями та корпораціями, сьогодні він вже не забезпечує потрібного рівня захисту (рівень безпеки його зменшується приблизно в 10 разів за рік).
- Третім, напевно, найперспективнішим варіантом є використання математичного апарата еліптичних кривих для реалізації алгоритму DSA (ECDSA).

ГОСТ Р 34.10–94 дуже подібний на DSA. Він передбачає використання односторонньої хеш-функції H(x) згідно з ГОСТом Р 34.11–94, що базується на симетричному алгоритмі ГОСТу 28147–89. Однак сьогодні відомі принаймні три слабкі місця в цьому стандарті, зокрема можливості:

- підміни повідомлення, якщо дозволено використання двох ключів;
- генерування слабкого підпису, що дозволяє навмисно компрометувати закритий ключ з метою відмови від наступних документів;
- генерування універсального цифрового підпису документа (незалежного від його хеш-коду) при певних значеннях параметрів алгоритму.

Отже, цей алгоритм є небезпечним і використовувати його фактично не можна.

2. Стійкість систем цифрових підписів

Основою криптоаналізу систем з відкритими ключами є відповідні алгоритми, які розв'язують базові проблеми криптографії з відкритим ключем, оскільки атака "грубою силою" (прямим перебором) в цих системах є практично нереальною. Ефективні алгоритми для вирішення першої проблеми вже створені. Формально неможливо довести, що у найближчий час не будуть розроблені достатньо швидкі алгоритми, які за прийнятний час (залежно від терміну використання ключів та важливості інформації) зможуть відновити ключ. Також можливе створення систем, матеріальні затрати на побудову яких (мільярди доларів в масштабах країни чи навіть однієї особи) будуть доцільними для реалізації даних задач.

Існують певні прогнози на необхідну довжину ключа на найближчі 15 років. Один з них, для алгоритму RSA, наведений в табл. 1та 2.

Таблиця 1

Доступна обчислювальна потужність з використанням Internet

Рік	Обчислювальна потужність
1998	$2x10^8$ MIPS
2008	$1.4x10^{10}$ MIPS
2018	$10^{13} – 10^{16}$ MIPS

Таблиця 2

Необхідна потужність для розкладання чисел за допомогою алгоритму NFS

Довжина в бітах	Обчислювальна потужність
512	$3x10^4$ MIPS
768	$2x10^8$ MIPS
1024	$3x10^{11}$ MIPS
1280	$1x10^{14}$ MIPS
1526	$3x10^{16}$ MIPS
2048	$3x10^{20}$ MIPS

Отже, сьогодні з врахуванням "закону" Мура та загальних темпів прогресу мінімальним безпечним ключем є ключ довжиною 1024 біти. Враховуючи найближчі потреби та швидкість впровадження складних систем в експлуатацію для новостворюваних систем цифрового підпису, необхідно забезпечити довжину ключа 2048 бітів.

3. Опис запропонованої системи

Основними структурними частинами системи є:

- інтелектуальна карта;
- точка з'єднання з глобальною мережею Internet, обладнана пристроєм для зчитування інтелектуальної карти;
- центр сертифікації.

Інтелектуальна карта призначена для проведення всіх операцій для електронного підписування документів. На її лицьовому боці розміщується фотокартка особи, її паспортні дані та група крові. Мікросхема смарт-карти містить закриті ключі особи та апаратну реалізацію алгоритмів обміну ключами та формування цифрового підпису (хеш-функції та криптосистеми з відкритим ключем). Це забезпечує додатковий рівень захисту, оскільки

закритий ключ після його запису в пам’ять смарт-карти ніколи не виходить за її межі. Як основний алгоритм для формування цифрового підпису пропонується використовувати алгоритм ECDSA. При довжині ключа 2048 біт та хеш-коду 160 біт цей алгоритм має достатню стійкість до всіх відомих методів криптоаналізу, причому він швидший за класичні алгоритми DSA та RSA.

Інтелектуальна карта не містить персональної інформації в електронній формі. Вона знаходиться в регіональних центрах сертифікації, отже, немає сенсу красти паспорт.

Для ефективної реалізації системи цифрового підпису в масштабах всієї країни потрібно забезпечити відповідну підтримку криптографічної системи з відкритим ключем – інфраструктури відкритих ключів (PKI). Вона передбачає забезпечення коректної генерації, сертифікації та розподілу ключів між об’єктами та суб’єктами інфраструктури відкритих ключів.

Для сертифікації та розподілу відкритих ключів використовується власний механізм цифрових сертифікатів, повністю сумісний з рекомендацією ITU–T X.509v3, оскільки вона фактично є світовим стандартом на цифрові сертифікати. Цифровий сертифікат містить інформацію про відповідний центр сертифікації та особу, якій видано сертифікат.

Точки з’єднання з глобальною мережею Internet призначені для передачі та прийому підписаних документів, отримання відкритого ключа відправника і верифікації цифрового підпису відправника. Як такі точки з’єднання може використовуватись весь наявний спектр відповідних засобів (персональні комп’ютери, ноутбуки та кишенькові комп’ютери, стаціонарні та мобільні термінали тощо). Однак на них має бути встановлене спеціальне програмне забезпечення. Окрім того, точки з’єднання повинні мати вбудований пристрій зчитування інтелектуальних карт або можливість підключення зовнішнього пристрою. Отже, сам пристрій може бути або вбудованим, або зовнішнім і працювати з іншими пристроями за одним із поширених протоколів.

4. Опис інтелектуальної карти

Інтелектуальна карта складається з таких вузлів (рис. 1):

– швидкого послідовного інтерфейсу;
– центрального процесора;
– криптографічного процесора;
– захищеної пам’яті даних та програм;
– відкритої пам’яті даних та програм.

Швидкий послідовний інтерфейс призначений для зв’язку із зовнішнім комп’ютером. Сучасні інтерфейси є порівняно повільними і не дозволяють обробляти документи всередині самої карти.

Центральний процесор керує роботою інтелектуальної карти. Він читає документ з послідовного порту і передає його на обчислення цифрового підпису у криптографічний процесор. Також він приєднує цифровий підпис до отриманого документа.

Криптографічний процесор прискорює виконання алгоритмів цифрового підпису. Він апаратно обчислює алгоритми шифрування з відкритим ключем та блокового шифрування, обчислення хеш-функції та електронного підпису.

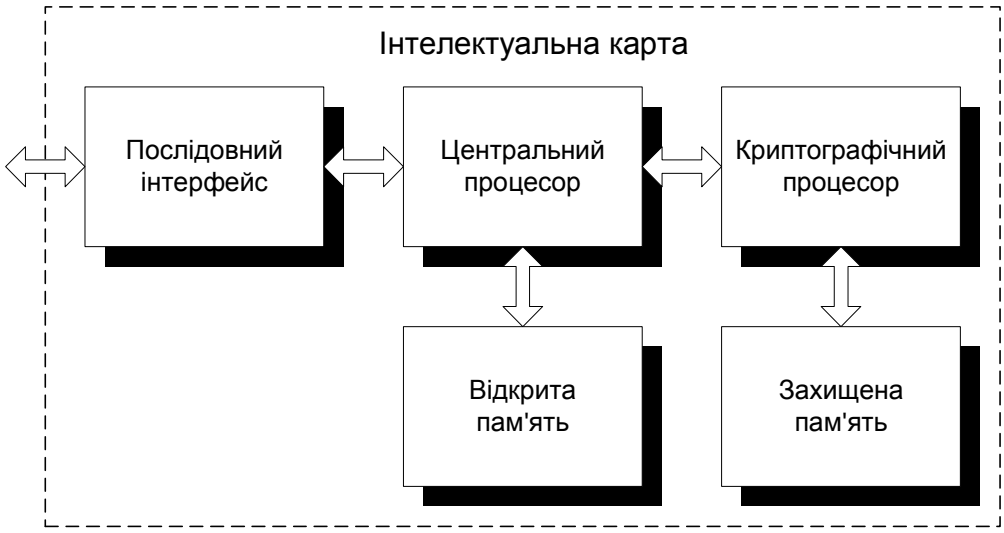

Рис. 6. Структура інтелектуальної карти

Основною перевагою даного варіанта інтелектуальної карти є повна обробка документа всередині карти, що не дає можливості проводити атаку на систему цифрового підпису шляхом зміни протоколу обчислення підпису для отримання закритого ключа.

5. Висновки

Отже, розробка інтелектуальної карти дає можливість впроваджувати в експлуатацію інформаційні системи, що використовують в своїй роботі цифровий підпис. Інтелектуальна карта дозволяє отримати високий рівень захисту при достатній для промислового використання швидкодії, універсальності та простоті використання. На основі запропонованої інтелектуальної карти можна розробити систему цифрового підпису, сумісну з міжнародними системами, побудовану на перевірених міжнародних алгоритмах. Виготовлення необхідного обладнання практично повністю можна реалізувати на українських підприємствах, що забезпечить вирішення питань конфіденційності та контролю за виготовленням.

1. Юргенсен Т., Гаттери С. Смарт-карты: настольная книга разработчика/ Пер. с англ. – М.: КУДИЦ-ОБРАЗ, 2003. – 416 с. 2. Schneier Applied B. Cryptography, Second Edition: Protocols, Algorithms, and Source code in C. 2. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – СПб.: БХВ–Петербург, 2000. – 320 с.: ил. 3. Молдовян Н. А. Проблематика и методы криптографии. – СПб.: Издательство СПбГУ. – 1998.