10. FIPS 180-1, "Secure Hash Standard", Federal Information Processing Standard (FIPS), Publication 180-1, National Bureau of Standards, U. S. Department of Commerce, Washington D. C. 11. R. Rivest. The MD4 Message-Digest Algorithm // Network Working Group, Request for Comments: 1320, April 1992. 12. R. Rivest. The MD5 Message-Digest Algorithm // Network Working Group, Request for Comments: 1321. 13. R. L. Rivest, A. Shamir, and L. M. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". Communications of the ACM, 21(2): 120–126, February 1978. 14. T. ElGamal, "A Public Key Cryptosystem and a Signature System Based in Discrete Logarithms", IEEE Trans. on Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985. 15. W. Diffie, M. Hellman New Directions in cryptography // IEEE Transactions on Information Theory, November 1976. 16. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с. 17. Бодров А. В., Коркишко Т. А., Молдовян Н. А. Программные шифры: пути повышения производительности // Материалы II Межрегиональной конференции "Информационная безопасность регионов России ИБРР-2001" (Санкт-Петербург, 26–29 ноября 2001). – 210 с., С. 86–87. 18. Мельник А. О., Коркішко Т. А. "Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів" //Вісник державного університету "Львівська політехніка" Комп'ютерні системи і мережі № 385, Львів, 2000, С. 77–81. 19. Мельник А. О., Аль-Кхатіб А. "Концепція побудови нарощуваних параметризованих процесорних ядер спеціалізованих надвеликих інтегральних схем" // Вісник Державного університету "Львівська політехніка" № 350, "Комп'ютерні системи та мережі", стор. 44–47. 20. M. Keating, P. Bricaud "Reuse Methodology Manual for System-On-a-Chip Design", Kluwer Academic Publishers, 1999, 224 p.

УДК 681.3

ПРОПОЗИЦІЇ З РЕАЛІЗАЦІЇ СИСТЕМИ ЦИФРОВИХ ПІДПИСІВ В УКРАЇНІ

Анатолій Мельник, Юрій Морозов, Володимир Сокіл
ТзОВ «Інтрон»

Анотація: **Розглядається варіант побудови системи цифрового підпису на основі інфраструктури відкритих ключів з використанням електронних паспортів.**
Summary: **In the paper the variant of construction of system of the digital signature is considered on the basis of an infrastructure of open keys with use the virtual passports.**
Ключові слова: **Цифровий підпис, цифровий сертифікат, алгоритми хеш-функцій, криптосистема з відкритими ключами, електронний паспорт.**

I Огляд систем цифрових підписів

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 сумірними з глобальними трагічними випадками.

В Україні широко впроваджуються інформаційні технології практично в усі галузі економіки. Все більша кількість організацій переходить на електронний документообмін. Отже, необхідними є кроки 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.

На 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 до деякої міри залежною від РФ. У 2001 році в РФ був прийнятий новий стандарт цифрового підпису. Отже, зараз Україні потрібна система для забезпечення інфраструктури цифрових підписів в 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. Він 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 широко вживаними 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 трьох проблемах:

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

$$g^x \equiv M (\mathrm{mod}\, p);$$

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

$$M^d \equiv C (\mathrm{mod}\, N);$$

– для заданих цілих чисел e та C знайти M, для якого

$$M^e \equiv C (\mathrm{mod}\, N);$$

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

$$x \equiv y^2 (\mathrm{mod}\, N).$$

Розглянемо коротко існуючі стандарти цифрового підпису на прикладі стандартів США FIPS PUB 186-2 (DSS) як відкритого та достатньо дослідженого, та діючого в 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 скінченому полі. Стандарт передбачає використання ключів довжиною від 512 до 1024 бітів. При довжині ключа 1024 біти 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 отримав дуже широке розповсюдження і підтримку багатьох світових організацій та корпорацій, на даний момент він вже не забезпечує потрібного рівня захисту (рівень безпеки його падає приблизно в 10 разів за рік).

– Третім, напевно самим перспективним, варіантом є використання математичного апарату 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 ГОСТ Р 34.11-94, що базується на симетричному алгоритмі ГОСТ28147-89. Однак на даний момент відомо принаймні три слабких місця в цьому стандарті:

– можливість підміни повідомлення, якщо дозволено використання двох ключів;

– можливість генерування слабкого підпису, що дозволяє навмисну компрометацію закритого ключа з метою відмови від наступних документів;

– можливість генерування універсального цифрового підпису документу (незалежного від його хеш-коду) при певних значеннях параметрів алгоритму.

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

II Стійкість систем цифрових підписів

Основою криптоаналізу систем з відкритими ключами є відповідні алгоритми, що 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 (в залежності від терміну використання ключів та важливості інформації) зможуть відновити ключ. Також є можливим 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 щодо необхідної довжини ключа у найближчі 15 років. Один з них, для алгоритму RSA, наведений в табл. 1 та 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, на даний момент з урахуванням "закону" Мура та згідно з загальними темпами 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 біт.

III Опис запропонованої системи

Основними структурними частинами системи є:

– електронний паспорт особи;

– точка з'єднання з глобальною мережею Internet, обладнана пристроєм для зчитування електронного паспорта;

– центр сертифікації.

Електронний паспорт особи – це інтелектуальна смарт-карта. На її лицьовій стороні розміщується фотокартка особи, її паспортні дані та група крові. Мікросхема смарт-карти містить закритий ключ особи та апаратну реалізацію алгоритмів обміну ключами і 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.

Електронний паспорт не містить персональної інформації в електронній формі. Вона знаходиться в регіональних центрах сертифікації. Це позбавляє сенсу крадіжку паспорта.

Авторизація та контроль за електронними паспортами покладається на відповідні обласні центри в системі відділів паспортизації Міністерства внутрішніх справ.

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 безплатне програмне забезпечення. Окрім того, точки з'єднання мають мати вбудований пристрій зчитування смарт-карт, або можливість підключення зовнішнього пристрою. Отже сам пристрій може бути або вбудованим, або зовнішнім і працювати з іншими пристроями за одним з поширених протоколів.

Для ефективної реалізації системи цифрового підпису в масштабах усієї 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.

Оскільки, згідно з чинним законодавством, основними документами, що посвідчують особу, є паспорт громадянина України, закордонний паспорт, посвідчення водія та військовий квиток, то сертифікат для кінцевого користувача містить відповідну інформацію з цих документів (номера паспортів, посвідчення водія та військового квитка, прізвище ім'я та по-батькові, біометричні дані, місце проживання тощо). Для забезпечення сумісності з X.509 вся додаткова інформація зберігається у відповідних некритичних розширеннях.

Згідно з рекомендацією ITU-T X.509v3 основною інформацією про центр сертифікації є його назва та відкритий ключ. Назва центра сертифікації має бути унікальною в межах цілої системи. Отже задача реєстрації та управління іменами центрів сертифікації покладається на центральний сервер сертифікації України.

При реалізації інфраструктури цифрових сертифікатів використовується схема з 2+ рівнів (рис. 1).

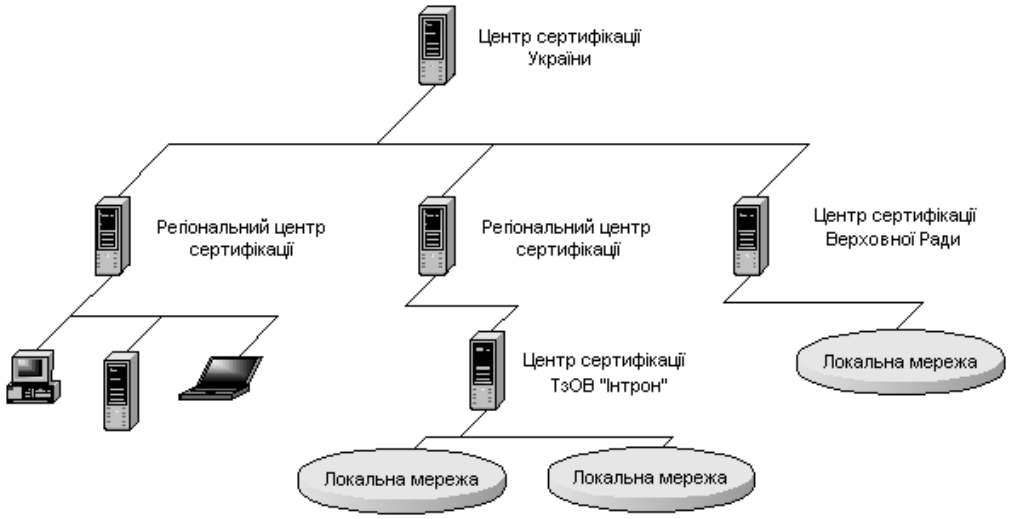

Рисунок 1 – Інфраструктура цифрових сертифікатів

На першому рівні знаходиться загальнодержавний центр (сервер) сертифікації. Він виконує сертифікацію регіональних серверів (наприклад, розподілених обласними центрами, або за будь-яким іншим принципом). Також він може, за потребою, обслуговувати певні державні структури.

В свою чергу регіональні сервери обслуговують якусь частину території України. Оскільки на них буде припадати найбільше навантаження, великим організаціям та установам рекомендується на третьому і нижчих рівнях створювати власні сервери сертифікації. Вони сертифікуються регіональними центрами. Невеликі організації та фізичні особи можуть безпосередньо користуватись послугами регіональних центрів сертифікації.

Ключі регіональних серверів та серверів нижчих рівнів генеруються на самому сервері і сертифікуються сервером вищого рівня. Для підвищення надійності та криптостійкості системи пропонується автоматична зміна ключів кожен рік.

IV Висновки

Створення національної системи цифрових підписів відповідає стратегічним інтересам України. Пропонується варіант реалізації такої системи, сумісний з міжнародними системами, побудований на перевірених міжнародних алгоритмах.

Система володіє достатньою для промислового використання швидкодією, універсальністю та простотою використання.

Розробка такої системи може бути здійснена в короткий термін та зі значною економією коштів на основі розробок ТзОВ "Інтрон". Виготовлення необхідного обладнання практично повністю можна реалізувати на українських підприємствах, що забезпечить вирішення питань конфіденційності та контролю за виготовленням.

Література: 1. B. Schneier. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source code in. С. 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.: издательствр СпбГУ. – 1998.

УДК 004.56.021.2: 510.22 (043.2)

КЛАССИФИКАЦИЯ НЕЧЕТКИХ ЧИСЕЛ ДЛЯ РАЦИОНАЛЬНОГО ПРИМЕНЕНИЯ В МЕТОДАХ И МОДЕЛЯХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Александр Корченко, Виктория Рындюк, Евгения Пацира
Национальный авиационный университет

Аннотация: **Предлагается классификация нечетких чисел для использования их в системах защиты информации.**
Summary: **The paper suggests a classification of fuzzy numbers for their using in information protection systems.**
Ключевые слова: **Нечеткие множества, нечеткие числа.**

I Введение

В области информационной безопасности существует множество задач [1–3], решение которых основано на методах и моделях теории нечетких множеств [4, 5], где, в частности, осуществляется обработка различных типов нечетких чисел (НЧ). Например, нечеткая логика применяется для измерения потенциальных потерь при анализе степени риска [6], при разработке методов принятия решений и оценки уровня защищенности компьютерных систем [7] и др.

II Постановка задачи

Исследуя известные методы выполнения операций с НЧ [8–15], приходим к выводу, что существует множество различных подходов к выполнению нечетких арифметических операций (НАО), каждый из которых рассчитан на определенный класс НЧ. К примеру, матричный метод с выбором строки и столбца с максимальным элементом, описанный в [9], пригоден для дискретных унимодальных НЧ. Метод выполнения монотонных операций над НЧ [11] рассчитан на непрерывные выпуклые НЧ. В последнее время появилось несколько новых методов выполнения НАО, но авторы не всегда однозначно определяют, какие же НЧ наиболее целесообразно и допустимо использовать. Такое положение во многом связано с тем, что в отечественной и зарубежной литературе до сих пор нет наиболее полной классификации НЧ, которые используются при выполнении НАО и, как следствие, область применения указанных методов была недостаточно определена. Учитывая указанные недостатки, в данной работе предлагается классификация НЧ, которые наиболее часто используются при решении разного рода прикладных задач, основанных на выполнении НАО.

III Основная часть

Многолетний опыт работы авторов в этом направлении показал, что классификацию НЧ лучше всего осуществлять по следующим признакам: по нормальности, модальности, выпуклости, непрерывности и параметричности. Раскроем сущность указанных признаков.

По нормальности НЧ можно разделить на нормальные и субнормальные.

Нормальные. НЧ $\underset{\sim}{X}$ на действительной прямой называется нормальным, если $\exists \mu_{\underset{\sim}{X}}(x_i) = 1 \ , (i = \overline{1,n})$

[8, 11, 16], т. е. верхняя граница значений его функции принадлежности (ФП) равна единице. Пример нормальных НЧ приведен на рис. 1.

Субнормальные. НЧ субнормально, если верхняя граница значений его ФП меньше единицы [11, 12, 15], т. е. $\max \mu_{\underset{\sim}{X}}(x) < 1$, где

$$\max \mu_{\underset{\sim}{X}}(x) = \bigvee_{i=1}^{n} \mu_{\underset{\sim}{X}}(x_i) < 1. \qquad (1)$$