Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ІВАНЕНКО ДМИТРО ВІКТОРОВИЧ

УДК 681.3.06

МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ СХЕМ НАПРАВЛЕНОГО ШИФРУВАННЯ В КІЛЬЦЯХ ЗРІЗАНИХ ПОЛІНОМІВ ДО АТАК СПЕЦІАЛЬНОГО ВИДУ НА РЕАЛІЗАЦІЮ

05.13.21 – системи захисту інформації

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.
Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор **Бондаренко Михайло Федорович**, Харківський національний університет радіоелектроніки, ректор Харківського національного університету радіоелектроніки

Офіційні опоненти: доктор технічних наук, професор **Краснобаєв Віктор Анатолійович,** Полтавський національний технічний університет імені Юрія Кондратюка, завідувач кафедри комп'ютерної інженерії;

кандидат технічних наук, доцент **Єсін Віталій Іванович,** Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій.

Захист відбудеться «24» 09 2013 р. о 15 годині на засіданні спеціалізованої вченої ради К 64.052.05 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, просп. Леніна, 14.

З дисертацією можна ознайомитися у бібліотеці Харківського національного університету радіоелектроніки (просп. Леніна, 14).

Автореферат розісланий «23» 08 2013 р.

Вчений секретар
спеціалізованої вченої ради І.В. Лисицька

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У інформаційному суспільстві найціннішим активом є інформація. Без ефективного використання інформаційних ресурсів неможливо уявити ні сучасне керування державою, ні розвиток бізнесу. Без інтенсивного обміну інформацією неможливо уявити сучасний фінансовий сектор. Людство всі більше покладається на автоматизовані системи керування. Тому однією з найбільших загроз можна визнати атаки на такі системи. Однією з основних функцій таких систем є обмін інформацією. Для забезпечення обміну інформацією потрібно виконувати наступні послуги безпеки: цілісність, автентичність, неспростовність, доступність, конфіденційність та надійність. Послуги причетності джерела та одержувача інформації (спостережливості) надаються за вимогами нормативних документів, міжнародних документів та міжнародних стандартів у сфері інформаційних технологій. Причетність джерела, тобто авторство, може бути забезпечено за рахунок застосування електронного цифрового підпису. Складніше забезпечити причетність одержувача. Ця задача може бути розв'язана за рахунок використання направлених шифрів. На сьогодні найбільш популярними криптосистемами є направлені шифри: RSA (абревіатура від прізвищ Rivest, Shamir і Adleman), ECC (elliptic curve cryptography, еліптична криптографія). Ці алгоритми пройшли перевірку часом та отримали визнання.

В роботі піднімається проблема ефективного захисту від несанкціонованого доступу інформації, що обробляється в інформаційних системах. Зараз для вирішення цієї проблеми використовуються схеми (далі метод) направленого шифрування (НШ) RSA та ECC, але з розвитком IT-технологій та ростом обчислювальної потужності і в цих алгоритмах можуть виникнути сумніви. RSA має субекспоненціальну складність, та для забезпечення допустимого рівня стійкості потрібно постійно збільшувати розмір модуля криптографічного перетворення та розмір ключів. Зростання розміру параметрів веде до підвищення складності, внаслідок чого буде зменшуватися швидкість обчислення. ECC має експоненціальну складність, математичний апарат алгоритму передбачає, що повідомлення має бути точкою на еліптичній кривій. Тобто у випадку класичного НШ перед зашифруванням блоки інформації необхідно подати у вигляді точок еліптичної кривої. Ця задача поліноміальної складності, але за складністю має такий самий порядок, що й шифрування, що зменшує швидкість НШ. Існують і інші методи НШ, але вони відносяться до комбінованих. Також недоліком загального алгоритму є дуже велика складність – для кожного блоку потрібно генерувати параметр та виконувати скалярне множення. Одним з перспективних методів НШ вважають алгоритм NTRU, про це свідчить факт, що у квітні 2011 року Американський комітет Accredited Standards Committee затвердив алгоритм шифрування NTRU як технічний стандарт у фінансових додатках. За словами Еда Адамса, виконавчого директора компанії Security Innovation, NTRU буде спроможний конкурувати з RSA та ECC. Схожий за принципом дії з RSA, NTRU має експоненційну та субекспоненційну складність та на 4 порядки швидше ніж RSA, та на 3 – ECC.

Робота зосереджена на дослідженні рівня безпеки метода НШ NTRU, аналізі імовірності успішності «класичних» атак на NTRU, та, при цьому, значна

увага приділяється атакам спеціального виду на реалізацію. Мова буде йти про більш повне вивчення й дослідження методів атаки спеціального виду (SPA, DPA, CPA), які базуються на аналізі енергоспоживання пристрою та оцінки складності їх реалізації на метод НШ NTRU. Вищезазначене і визначає актуальність теми та досліджень цієї роботи.

Зв'язок роботи з науковими програмами, темами. Дисертаційна робота виконана в рамках держбюджетної НДР № 262-1 "Розвиток, стандартизація, уніфікація, удосконалення та впровадження інфраструктури відкритих ключів, включаючи національну систему електронного цифрового підпису (ЕЦП)" за наказом МОНУ № 1177 від 30.11.2010 (ДР № 0111U002628) та госпдоговірної НДР № 11-06 від 01.03.2011р. "Розробка методів, комплексів та засобів інфраструктури відкритих ключів (ІВК) для національних та міжнародних інформаційно-телекомунікаційних систем та інформаційних технологій" (ДР № 0111U002634).

Мета та задачі дослідження. Метою досліджень є аналіз якості існуючих, удосконалення та розробка нових методів протидії атакам спеціального виду на реалізацію для схем (далі – метод) НШ у кільцях зрізаних поліномів (далі – на решітках).

Для досягнення поставленої мети в роботі вирішені наступні основні задачі:

— Проведення аналізу існуючих та перспективних методів НШ, визначення критеріїв та показників, порівняльна характеристика. Визначення та обґрунтування вимог до криптоперетворень у епоху постквантової криптографії.

— Аналіз існуючих основних алгоритмів теорії решіток. Аналіз математичної моделі криптосистеми NTRU.

— Проведення аналізу рівня безпеки метода НШ на решітках на імовірність «класичних атак» та атак спеціального виду на реалізацію.

— Удосконалення метода НШ на решітках з метою захисту від атак спеціального виду на реалізацію першого роду, яка базується на підрахуванні кількості звернень до геш-функції та отриманні додаткової інформації (час обчислення геш-функції), шляхом використання додаткових додавань (додаткові звернення до геш-функції).

— Проведення аналізу складності реалізації ефективної (успішної) атаки спеціального виду на реалізацію, визначення методики оцінки складності реалізації атаки спеціального виду.

— Аналіз стійкості метода НШ на решітках до атак спеціального виду на реалізацію, які базуються на аналізі енергоспоживання пристрою під час обчислення операцій алгоритму.

— Аналіз існуючих методів протидії атакам спеціального виду на реалізацію, які базуються на аналізі енергоспоживання пристрою, оцінка складності реалізації успішної атаки.

— Розробка методу протидії атакам спеціального виду, які базуються на аналізі енергоспоживання пристрою, з метою підвищення стійкості метода НШ на решітках. Оцінка ефективності розробленого методу.

Об'єктом досліджень є процеси зашифрування та розшифрування методи НШ на решітках, де домінуючими операціями є операції згортки та добутку, звернень до геш-функції.

Предметом досліджень є методи підвищення стійкості методів НШ на решітках до атак спеціального виду на реалізацію.

Методи досліджень спираються на використання теорії решіток для аналізу основних алгоритмів НШ на решітках для подальшого криптоаналізу; теорії ймовірності та математичної статистики під час дослідження показників оцінки складності реалізації атаки спеціального виду, які базуються на аналізу спектру енергоспоживання; методів статистичних випробувань під час виконання експериментальних досліджень кореляції спектру енергоспоживання пристрою, на якому обчислювався алгоритм NTRU; дерева прийняття рішень під час виконання експериментальних досліджень методів протидії та оцінки складності атак спеціального виду; метода визначення вагових коефіцієнтів на основі функції втрати ефективності систем при порівняні сучасних методів НШ.

Наукова новизна отриманих результатів дисертаційної роботи. У дисертаційній роботі отримано теоретичне узагальнення та нове вирішення важливого науково-технічного завдання підвищення стійкості методам НШ. Отримано такі нові наукові результати:

1) Вперше розроблено метод протидії атакам спеціального виду, який відрізняться від відомих використанням операцій рандомізації тимчасових даних t та масиву b, одночасно, що дозволяє ускладнити можливість відновлення конфіденційної інформації при аналізу спектру енергоспоживання.

2) Вперше сформовано перелік вимог для метода НШ, який відрізняється від відомих тим, що враховує аспекти криптографічної стійкості за умови появлення квантових комп’ютерів.

3) Удосконалено модель програмно-апаратної реалізації алгоритму NTRU, яка відрізняється від відомих використанням додаткових додавань, що дозволить ускладнити реалізацію атаки спеціального виду, які базуються на аналізі спектру енергоспоживання пристрою та часу обчислення операції.

Практичне значення отриманих результатів полягає у тому, що:

– Розроблено обчислювальні алгоритми і удосконалено програмно-апаратну реалізацію геш-функції для алгоритму NTRU за рахунок використання додаткових «додавань» (звернень до геш-функції), що дозволить мати однакову стійкість з відомими методами, але вигравати у швидкості – майже на 9%;

– Отримані практичні результати стійкості програмно-апаратної реалізації алгоритму NTRU до атак спеціального виду на реалізацію, які базуються на аналізі спектру енергоспоживання. Запропонований метод протидії дозволить збільшити потрібну кількість блоків повідомлення, яку буде потрібно порушнику для винесення припущення щодо значення конфіденційної інформації. Результати впроваджено в діяльність ПАТ «Інститут інформаційних технологій », що підтверджено відповідним актом впровадження (акт від 15.10.2012р.);

— Отримані практичні результати порівняння перспективних методів НШ на основі запропонованого переліку вимог, які дозволили визначити, що NTRU краще за RSA та ECC в 6 разів, ECC гірше за RSA в 1.04 рази. Результати

впроваджено в науковий процес на кафедрі безпеки інформаційних технологій в Харківському національному університеті радіоелектроніки, що підтверджено відповідним актом впровадження (акт від 19.10.2012р.).

Особистий внесок здобувача. У роботах, які написані у співавторстві, автору належить: [1,8] – визначення проблемних питань електронної автентифікації; [2, 7, 10] – аналіз основних аспектів механізмів автентифікації смарт-карт; [3] – удосконалення метода НШ за показником нерозбірливості спектру енергоспоживання пристрою; [4] – аналіз сучасних асиметричних криптосистем; [14-16] – дослідження атак спеціального виду на реалізацію, що використовують CPA та SPA методи, на апаратну реалізацію метода НШ; [9, 11-13] аналіз систем захисту від несанкціонованого доступу.

Апробація результатів дисертації. Основні результати дисертаційної роботи були представлені, доповідалися й обговорювалися на міжнародних і всеукраїнських науково-технічних конференціях, зокрема на: IV міжнародній конференції молодих вчених, CSV-2010 (м. Львів 2010р.); на 13-й, 15-й міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах»(м. Київ, 2010р.; м. Київ, 2012р.); на 14-му, 15-му ювілейному міжнародному молодіжному форумі «Радіоелектроніка і молодь в XXI столітті» (м. Харків, 2010р.; м. Харків, 2011р.); на науково-технічній конференції з міжнародною участю «Комп'ютерне модулювання в наукомістких технологіях», КМНТ - 2010 та КМНТ - 2012 (м. Харків, 2010р.; м. Харків, 2012р.); на VI всеукраїнській студентській науково-практичній конференції. «Наукові дослідження молоді — вирішенню проблем європейської інтеграції.» (м. Харків, 2011р.);на II міжнародній науково-практичній конференції молодих вчених «Інфокомунікації – сучасність та майбутнє» (м. Одеса, 2012р.).

Публікація результатів роботи. Основні положення та результати дисертаційної роботи опубліковано у 16 наукових працях: 6 статей у фахових виданнях України з технічних наук (з них 2 одноосібні) та 10 публікацій матеріалів і тез доповідей на міжнародних науково-технічних конференціях.

Структура та обсяг дисертації. Дисертація складається із вступу, п'яти розділів і висновків, має обсяг 181 сторінка, з яких 150 сторінка основного тексту, які містять 48 рисунків, 14 таблиць (рисунки та таблиці, що займають площу на 10 сторінках), список використаних джерел із 84 найменувань на 9 сторінках та 2 додатки на 9 сторінках.

ОСНОВНИЙ ЗМІСТ

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, сформульовано основну мету і задачі дослідження, наведено відомості про зв'язок обраного напрямку досліджень із планами організації, де виконана робота. Надано стислу анотацію отриманих у дисертації рішень, визначено їх практичну цінність, наведено дані про використання результатів досліджень.

У **першому розділі** розглядається сутність основних методів НШ: НШ в кільці (RSA - перетворення), НШ в полі Галуа F(p), НШ в групі точок еліптичних

кривих $E(F(q))$, НШ на решітках. Формується задача визначення перспективного методу НШ за умови створення у майбутньому квантового комп'ютера. Внаслідок чого було проаналізовано складність алгоритмів та задач теорії решіток та розглянута загальна криптографія на решітках. Проаналізовано джерела відносно криптосистем на основі решіток.

Робиться висновок, що криптографічні примітиви та протоколи, які основані на задачах теорії решіток, є надзвичайно перспективним напрямом в області постквантової криптографії. Багато з них достатньо ефективні та можуть конкурувати з найкращими з відомих альтернатив, так що вони, як правило, достатньо прості в реалізації

В досліджені стисло відмічаються перспективи використання методів НШ на решітках, NTRU, тому напрямок досліджень цієї роботи визначається актуальним - порівняння сучасних методів НШ, визначення перспективного методу та детального дослідження методу НШ з метою визначення можливих вразливостей та недоліків.

Наводиться понятійний апарат теорії решіток. Визначаються такі поняття, як решітка L, ранг решітки, лінійно незалежні вектори $\left\{\overline{b_1},...,\overline{b_n}\right\} \subset R^m$, базиси решітки, найкоротший вектор решітки $\lambda(L) = \min\limits_{x,y\in L, x\neq y} \|x-y\| = \min\limits_{x\in L, x\neq 0} \|x\|$, ідеальна решітка.

Розділ завершується формулюванням висновків по проведеним дослідженням, а також формулюванням задач досліджень роботи.

Другий розділ присвячено аналізу основних криптоперетворень НШ, виявляються показники та залежності характеристик. З метою визначення кращої криптосистеми наводиться два метода прийняття рішень: метод ієрархій та метод визначення вагових коефіцієнтів на основі функції втрати ефективності системи. Метод визначення вагових коефіцієнтів на основі функції втрати ефективності системи оперує тільки кількісними показниками, тому зроблено висновок, що для більш точнішої відповіді при порівнянні потрібно використовувати саме цей метод.

Порівняння криптосистем НШ за допомогою метода визначення вагових коефіцієнтів привело до наступних результатів (див. рис. 1): криптосистема NTRU має значну перевагу перед криптосистемами RSA та ECC, приблизно у 6 разів, різниця між ECC та RSA незначна.

Визначивши кращу криптосистему, більш детально проаналізували криптосистему NTRU: описали загальні параметри; розглянули сутність алгоритму шифрування. Це дозволило вивчити та уточнити практичні аспекти криптографії на основі решіток, використання при побудові та криптоаналізі примітивів та протоколів, які базуються та задачах теорії решіток.

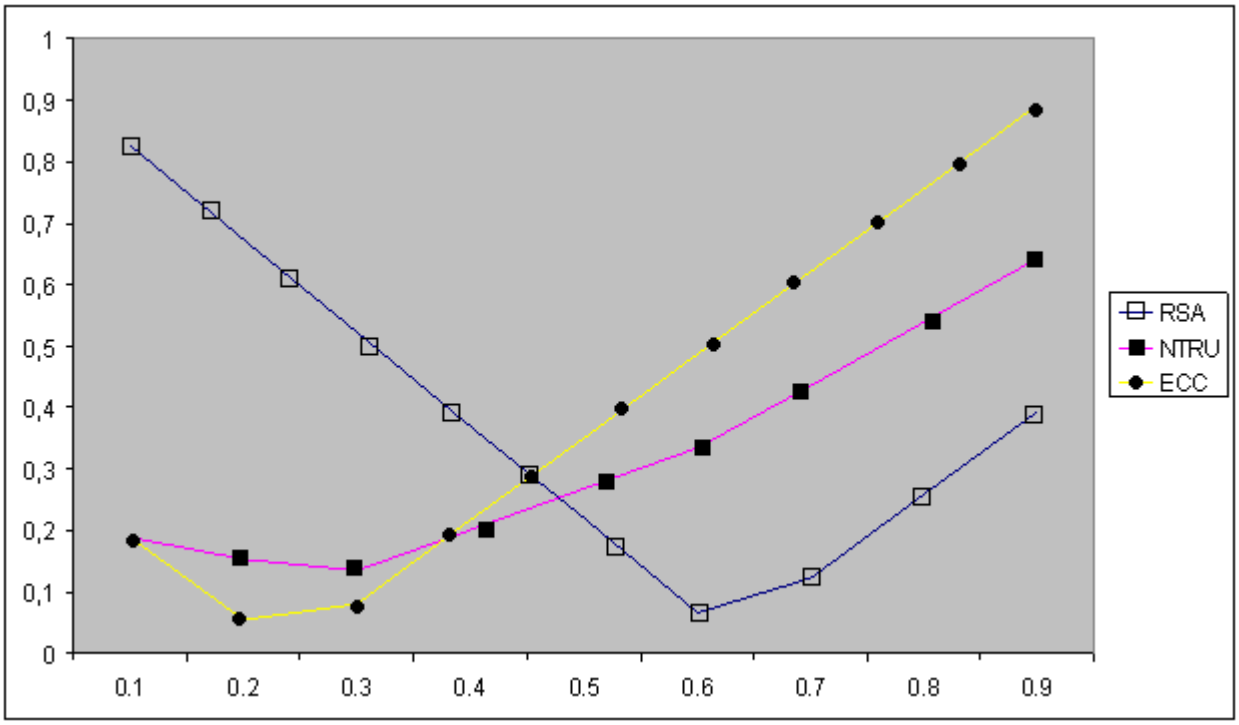

Рисунок 1 – Результат порівняння криптосистем НШ

Визначивши перспективну криптосистему на місце майбутнього національного стандарту, виникає задача дослідження, яке буде присвячене оцінці ступеня захищеності криптосистеми від сучасних атак, шукаючи найбільш ефективні, та оцінці складності реалізації самих атак. Наводиться класифікація сучасних атак:

— атаки «груба сила»(повного перебору);
— атаки з використанням квантового комп’ютера;
— аналітичні атаки:
  1) атаки з підібраним шифр-текстом;
  2) атаки пошуку найкоротшого вектору;
  3) атаки з адаптивно підібраним шифр-текстом;
  4) атаки з неправильно вибраними параметрами;
  5) атаки з «decryption failures».

Відкритих відомостей у розвитку квантових алгоритмів на даний час немає, тому в цій дисертаційній роботі атаки з використанням квантового комп’ютера не розглядалися.

У висновках зазначається, що криптосистеми, які побудовані на основі теорії решіток, мають більш високу стійкість до криптоаналізу, тому подальше використання не можливе без дослідження основних алгоритмів теорії решіток.

У **третьому розділі** досліджується ефективність сучасних атак на криптосистему NTRU. Одна зі складностей NTRU полягає у значній кількості варіації, різний набір параметрів повністю змінює властивості алгоритму. Тому для проведення досліджень було взято NTRU-1998, NTRU-2001, NTRU-2005.

Основні атаки на NTRU використовують «неоднозначність» процесу розшифрування, можливість виникнення неспівпадання розшифрованого повідомлення з повідомленням, яке зашифровувалося, при успішному розшифруванні.

У роботі розглянуті результати дослідження Howgrave-Graham, атаки з використанням «decryption failures» - атака на відновлення ключа для будь-якої схеми заповнення. Howgrave-Graham стверджує що, якщо отримати мільйон «decryption failures», то є можливість відновити багаточлен $X^N f(X) f(\frac{1}{\dots})$ і тоді можна відновити секретний ключ за допомогою алгоритма Gentry та Szydlo. Основна перевага цієї атаки полягає в тому що, так як усі повідомлення будуть генеровані валідно, атака сумісна з усіма версіями криптосистеми. Кількість в один мільйон «decryption failures» є тільки евристичною оцінкою, алгоритму Gentry та Szydlo для відновлення f з $X^N f(X) f(\frac{1}{\dots})$ за теоретичними оцінками атаці буде достатньо поліноміального часу, на практиці алгоритм реалізований не повністю.

Також у роботі представлені результати досліджень Gama та Nguyen, автори стверджують, що для повного відновлення секретного ключа достатньо декілька сотень «decryption failures», відповідно час дії дуже малий в порівнянні з часом збору необхідної кількості «decryption failures». Ідея алгоритма полягає в тому, щоб побудувати апроксимацію з вектором секретного ключа, чим більше використовується «decryption failures» для атаки, тим більше точність апроксимації. Оскільки секретний ключ має цілі коефіцієнти, апроксимація в кінцевому підсумку досягне такого рівня точності, на якому можна повністю відновити ключ. Практичні результати наведені у таблиці 2.

Таблиця 2 – Результати дослідження Gama та Nguyen

Версія NTRU	N	p	q	d_f	Кількість використаних «decryption failures»	Кількість відновлених бітів f
NTRU-1998	167	3	128	32	50 100	$N-3$ N (всі)
NTRU-2001	251	X+2	127	40	80 140	$N-1$ N (всі)
NTRU-2005 двійковий (зі зменшеним q)	251	2	127	64	80 130	$N-2$ N (всі)
NTRU-2005 похідної форми (зі зменшеним q)	251	2	113	9	100 150	$N-3$ $N-1$

Атака на решітку ґрунтується на пошуку найкоротшого вектору в конкретній решітці. Для розкриття особистого ключа $(f(x), f_p(x))$ порушнику потрібно побудувати матрицю, далі з рядків матриці потрібно побудувати решітку. Оскільки матриця буде містити відкритий ключ, то решітка буде містити й вектор (найкоротший вектор у заданій решітці). Знаходження такого вектора і є умовою зна-

ходження особистого ключа. Вважається, що визначення найкоротшого вектору в решітці є експоненційно складною задачею. В роботі були розглянуті результати дослідження D. Han (див.табл.3).

Таблиця 3 – Практичні результати атаки на решітку D. Han

N	67	107	139	167	191	221	251
q	61	101	131	157	181	211	239
d_f	19	31	40	48	55	63	72
T	24	49	75	102	124	151	177
T_{int},c	5.2	73.8	352	1117,3	2499,7	5872	12287,6
T_{red},c	1.9	17.9	57.9	144,1	195,4	317,2	460,8
T_{one},c	7.1	91.7	409.9	1261,4	2695,1	6189,2	12748,4
T_{tot},c	$2^{26.8}$	$2^{55.5}$	$2^{83.3}$	$2^{110.6}$	$2^{132.4}$	$2^{158.3}$	$2^{183.7}$

T_{int} є середнім значенням витраченого часу на побудування решітки £J$_t$ та T_{red} – середнє значення часу витраченого на алгоритм редукції по знаходженню цільового вектора. T_{one} - це сума T_{int} та T_{red}, яка відображає витрачений час на атаку у випадку, якщо коректно передбачені всі t біт повідомлення. Нарешті, T_{tot} - загальний час для успішної атаки оцінюється за наступною формулою:

$$T_{tot} = T_{one} \times \text{the number of predition} = T_{one} \times \sum_{i=0}^{d} tC_i \qquad (1)$$

З наведених результатів стало зрозуміло, що вище описана атака є успішною. Більше того, з великою імовірністю цю атаку можна провести у випадку, коли порушник розпаралелить обчислення - витрачений час на атаку буде пропорційно зменшуватися у відповідності до збільшення обчислювальних ресурсів.

Далі розглядаються атаки спеціального виду за наступними ортогональними признаками: контроль над обчислювальним процесом, спосіб доступу до системи, використаний метод атаки. Робиться припущення, що атаки спеціального виду, набуваючи розвитку і широкого розповсюдження, будуть найбільш ефективними, за рахунок використанням на свою користь людського фактору (помилки при розробці) та апаратних обмежень при програмно-апаратній реалізації.

У висновках наведено результати досліджень, пропонується використання NTRU як національного стандарту, формулюється задача дослідження проблемних питань та можливих вразливостей у програмно-апаратній реалізації алгоритму NTRU.

Четвертий розділ роботи присвячений більш детальному розгляду атак спеціального виду на енергоспоживання (див. рис. 2). Сутність атак спеціального виду, які базуються на аналізі енергоспоживання, полягає у тому, що число задіяних бітів у обчисленні операції пропорційно енергоспоживанні пристрою під

час цього ж обчислення. Для аналізу спектру енергоспоживання існує два метода: метод «код Хемінга», який припускає, що число задіяних бітів пропорційно енергоспоживанню пристрою і виражено як $HW(R) = popcnt(R)$; метод «відстань Хемінга», який припускає, що кількість змін стану бітів пропорційна енергоспоживанню пристрою, вимагає знання минулого та теперішнього стану пристрою, описується як OR двох станів так і $HW(R_0 + R_1)$.

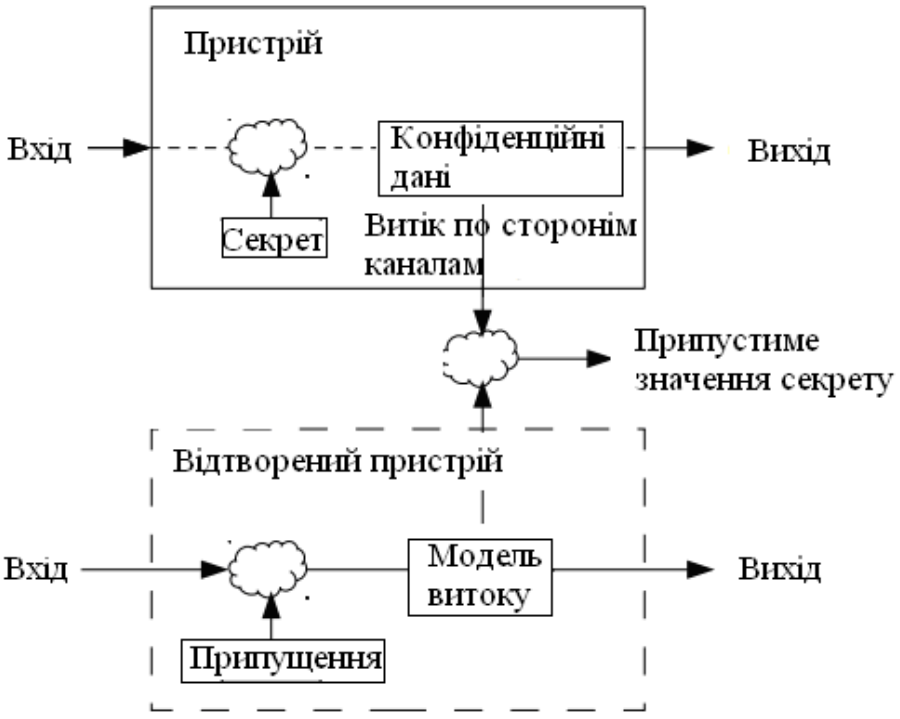

Рисунок 2 – Атака спеціального виду на енергоспоживання

Звертається увага на рівень та кваліфікацію порушника, розглядаються засоби та інструменти порушника. Для більш правдивих та точних результатів обираються інструменти, які безпосередньо використовують розробники програмно-апаратних реалізацій: Synopsys Design Compiler, Synopsys VCS, Synopsys PrimePower.

Далі розглядається можливість атака спеціального виду з використанням SPA, DPA та CPA методів. Завдання атаки зводиться до спостереження виконання операції згортки $F * e \bmod q$ та вимірювання порушником миттєвого енергоспоживання пристрою, заміряється різниця між можливими елементами, потім порушник робить припущення про значення. Робиться висновок, що для успішної реалізації атак спеціального виду з використанням методу SPA порушнику потрібно відстежити операцію згортання над одним блоком повідомлення.

Завдання атаки спеціального виду з використанням DPA та CPA методів полягає у спостереженні за найменшими змінами у енергоспоживанні між відповідними операндами та значеннями, та аналізі отриманих результатів, використовуючи код Хемінга та відстань Хемінга для. Для цього повідомлення має бути представлене у вигляді багаточлену S, множина $c^1, c^2, ..., c^S$, та мати сліди енерго-

споживання P, множина $P^1, P^2, ..., P^S$, які були залишені пристроєм при виконані операції над $c^1, c^2, ..., c^S$. Потім порушник робить припущення щодо значення при $w > 1$, та вираховує для кожного значення відстані Хемінга $D^l = HD(c_w^l, c_w^l + c_0^l)$ при $1 \le l \le S$. Наступний крок – це перевірка на наявність якої-небудь кореляції між D^l та P^l. Для вирішення цієї мети обчислимо коефіцієнт кореляції Пірсона, який допоможе виявити зміни між D^l та P^l:

$$P_{P,D}^t = \frac{\sum_{t=1}^{S}(P^l - \overline{P}) \cdot (D^l - \overline{D})}{\sqrt{\sum_{t=1}^{S}(P^l - \overline{P})^2 \cdot \sqrt{\sum_{t=1}^{S}(D^l - \overline{D})^2 \cdot}}}, \quad (2)$$

де $\overline{D}$ та $\overline{P}$ середнє значення D^l та P^l взяте у S випадках, відповідно. Відмітимо, що (2) може бути обчислена незалежно для кожного відповідного шагу t між слідами енергоспоживання. У випадку наявності значимої кореляції між P^l та D^l для деякого t означає, що $b[1] - b[0] = w$ коректне припущення (див. рис.3), та це t відповідає моменту, коли $c_{b[1]-b[0]} + c_0$ обчислюється. Тому завдання порушника полягає у знаходженні максимального значення вихідного w. Знайшовши значення $b[1] - b[0]$, інші значення знаходяться аналогічним методом. Після знаходження всіх відповідних зсувів $b[1] - b[0], ..., b[d-2] - b[d-1]$ останнім завданням буде знаходження вихідного $b[0]$ методом перебору.

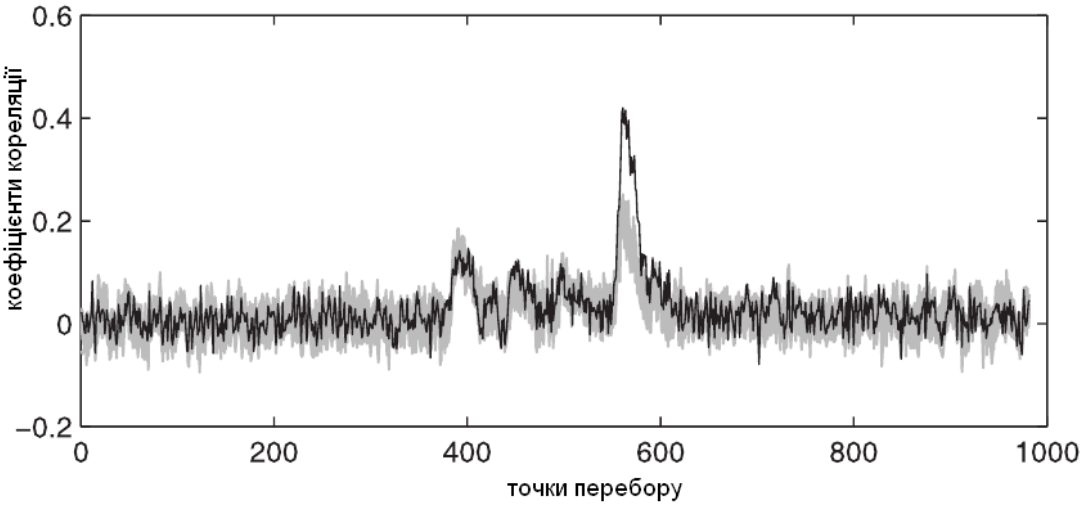

Рисунок 3 - Кореляція між енергоспоживанням та відстанню Хемінга на всі можливі припущення

Для реалізації цієї атаки порушнику буде потрібно перехватити одну операцію згортання та всі сліди енергоспоживання, відповідно.

DPA відрізняється від CPA тим, що обчислює відстань між двома середніми слідами A_1 та A_0, де A_1 – середнє значення, коли функція D (операція) вертає 1, та A_0 – коли функція D (операція) вертає 0. Кожен слід A_i має вигляд $T_{1...m}[1...k]$

$$\Delta_D[j]=\frac{\sum_{i=1}^{m} D(C_i,b,K_s)T_i[j]}{\sum_{i=1}^{m} D(C_i,b,K_s)}-\frac{\sum_{i=1}^{m}(1-D(C_i,b,K_s))T_i[j]}{\sum_{i=1}^{m}(1-D(C_i,b,K_s))}. \quad (3)$$

Далі розглянута програмна реалізація алгоритму NTRU, за допомогою метода SPA та Synopsys PrimePower стала відома додаткова інформація про хеш-функцію, що дало можливість розглянути таку ситуацію, коли є дві сторони А та Б, які обмінюються інформацією. Б – це порушник, який намагається дізнатись секретний ключ А. Порушник отримав додаткову інформацію (час обчислення, кількість звернень до хеш-функції). Порушник вибирає множину ε (шифр-текст), яка є набором багаточленів за $\bmod q$, та таке повідомлення М, щоб воно складалося з множини повідомлень створених А:

$$\{((f\cdot e \bmod q)\bmod 2\cdot(f^{-1}\bmod 2): e\in\varepsilon\}. \quad (4)$$

Припускаємо, що імовірність того, що наведене повідомлення, створене А, буде знайдено у множині М дуже велика. Б проводить атаку, створює список-пошук бінарного вектору, будує таблицю для кожної пари $M\times\varepsilon$:

$$(T(m',e)): m\in M,\ e\in\varepsilon. \quad (5)$$

Б посилає А деяке випадкове $e\in\varepsilon$. Коли шифр-текст буде відправлений, Б починає записувати, як довго А буде розшифровувати цей шифр-текст. Навіть коли відправлено підроблений шифр-текст, успішна перевірка буде відхилена. Порушник пов'яже часову інформацію з кількістю звернень до хеш-функції. Він буде знати значення $m'(e)$, яке може бути представлене у вигляді:

$$((f\cdot e \bmod q)\bmod 2)\cdot(f^{-1}\bmod 2). \quad (6)$$

Б не відомо значення $m'(e)$. Він знає тільки значення $\beta(m'(e),e)$ яке буде використовуватися після того, як буде порівняно зі значеннями отриманими від А, попередньо вирахуваними та записаними у таблицю, яка була створена Б. Для цього Б потрібно зробити $N-1$ записів. Ці значення він отримає після відправлення одного за іншим наступних багаточленів:

$$Xe, X^2e, X^3e, ..., X^{N-1}e\ . \quad (7)$$

Після відправки шифр-тексту, порушник отримає значення $\beta(m'(X^ie),X^ie)$. Візьмемо випадкове $m'(X^ie)$. Нехай відомо значення $m'(e)$ тоді можна застосувати це й до виразу $m'(X^ie)$ також:

$$m'(X^ie)=\left(\left(f\cdot X^ie \bmod q\right)\bmod 2\right)\cdot\left(f^{-1}\bmod 2\right), \quad (8)$$

оскільки усі X дорівнюють 0 чи 1, ми можемо взяти таке X^i та отримаємо

$$X^i\cdot((f\cdot e \bmod q)\bmod 2)\cdot\left(f^{-1}\bmod 2\right), \quad (9)$$

що насправді $X^im'(e)$.

Б знає функцію атаки $T(m'(e),e)$ від $(m'(e),e)$. На наступному етапі повинен відбутись пошук у сформованому списку, у якому з високою імовірністю знаходиться невелика кількість можливих пар із отриманих Б пар. Б має два багаточлена e, m', де А розшифровує *e* за допомогою багаточлена m'. З цього порушник вираховує тільки $m'\cdot f\equiv\left(f\cdot e \bmod q\right)\bmod 2$, де e та m' він знає.

У висновках відмічається, що для усунення вад, які виникли при атаці, потрібно використовувати додаткові «додавання», що ускладнить візуальний аналіз (метод SPA) спектру енергоспоживання та збільшить час обчислення алгоритму тільки на 9%.

У **п'ятому розділі** ставиться задача практичного дослідження програмно-апаратної реалізації алгоритму NTRU, методів протидії атакам спеціального виду на реалізацію пошук універсального методу протидії атакам спеціального виду на реалізацію.

Аналіз операцій зашифрування та розшифрування алгоритма NTRU, дозволив встановити, що домінуючими операціями є обчислення згортання $r * h \bmod q$ та $f * e \bmod q$. Оптимізований алгоритм представляє собою $t = a * c \bmod q$ (див. алгоритм 1), де приведення за модулем $\bmod N$ відбувається за рахунок використання додаткової пам'яті $(t_N,...,t_{2N-1})$, пересуваючись по індексу обчислення в масиві t. $a \in R$ є бінарним багаточленом з d ненульовими коефіцієнтами та $c \in R$ є загальним багаточленом. Бінарний багаточлен a представляє собою масив b, у якому позначено ненульові положення d:

Алгоритм 1 – Виконання операції згортання

Вхідні дані: b (масив, який представляє собою не нульові значення бінарного багаточлену $a(X)$); $c(X)$ (багаточлен).

Вихідні дані: $t(x)$.

1. for $0 \le j < 2N$ do
2. $t_j \leftarrow 0$ //з t_N до t_{2N-1} : тимчасовий буфер
3. end for
4. for $0 \le j < d$ do
5. for $0 \le k < N$ do
6. $t_{k+b[j]} \leftarrow t_{k+b[j]} + c_k$
7. end for
8. end for
9. for $0 \le j < N$ do
10. $t_j \leftarrow (t_j + t_{j+N}) \bmod q$
11. end for

Далі розглядається можливість атаки спеціального виду з використанням SPA, DPA та CPA методів, виявляються вразливості та недоліки алгоритму, що призводить до необхідності проаналізувати та розробити нові методи протидії. Тому далі приводиться низка існуючих методів протидії, робиться висновок, що рандомізація та засліплення даних є простими та ефективними методами протидії атакам спеціального виду, які базуються на аналізі енергоспоживанні. Раніше було зазначено, що операція згортання $t(X) = c(X) + a(X)$ є домінуючою, тому справедливо було запропоновано наступні методи протидії:

1) рандомізація тимчасових даних, які зберігаються у t;
2) засліплення відкритих даних c;
3) рандомізація секретних даних b.

Особливість криптосистеми NTRU встановлює обмеження на вибір r (випадкова зміна, яка буде додаватися у рамках рандомізації), t повинно задовольняти вимозі $t_{max} \le d \times max_{0 \le k < N} c_k$, де t_{max} - є максимумом серед t при $0 \le j \le 2N$. Тому просте узагальнення спостереження для інших значень призведе до припущення, що $r_j \le t_{max}$, якщо $max_{0 \le k < N} c_k$ у звичайному шифр-тексті, то $r_i < dq$. У випадку, коли порушник збере достатньо статистичних даних маючи випадки, коли $r_{b[1]} = r$, тоді стани будуть відігравати роль шуму, тому атака буде успішною без істотного збільшення числа потрібних слідів енергоспоживання.

Засліплення відкритих даних c може відбуватися двома варіантами за допомогою цілих чисел та багаточлену. Перший реалізує рандомізацію цілого r та неодноразово використовується для засліплення всіх c_k. Цей захід протидії маскує кореляцію між багаточленом c(X) та енергоспоживанням рандомізованого c(X). Насправді, ця процедура має наступний вигляд $(c(X) + R(x)) * a(X) - R(X) * a(X)$, де $R(X) = [r, r, ..., r]$. Тому що $R(X) * a(X) = [d_r \bmod q, d_r \bmod q, ..., d_r \bmod q]$, можемо ліквідувати $R(X) * a(X)$ шляхом віднімання d_r від кожного t_j. Другий метод оснований на використанні загального багаточлену R(X), який безпосередньо і буде засліплювати c(X). Потрібно вирахувати $(c(X) + R(x)) * a(X) - R(X) * a(X) = c(X) * a(X)$, спочатку обирається випадковий багаточлен *R(X)*, обчислюється $S(X) = R(X) * a(X)$ та зберігається R(X) та S(X). Коли згортка $(c(X) + R(x)) * a(X) - S(X)$ буде зроблено, R(X) та S(X) оновлюється шляхом обчислення $R(X) \leftarrow kR(X)$ та $S(X) \leftarrow kS(X)$ для випадкового k. Тому можна використовувати другий метод як ефективну протидію проти CPA, але засліплення *c* все одно не перешкодить реалізації SPA атаки.

Під час спостережень за поведінкою алгоритму виявився цікавий факт, що зміна порядку елементів множини b не впливає на результат операції згортання, що приховає позиції відносних зсувів – це дозволить запобігти атаці CPA. Але відстеживши одну операцію згортання та зробивши декілька успішних припущень, використовуючи дерево пошуку (див. рис. 4), порушник успішно реалізує атаку SPA.

Таким чином, порушник, зібравши статистичні дані, отримавши імовірнісну залежність зсувів при операції згортання багаточленів з використанням вектора рандомізації r_k, зведе нанівець розглянуті методи протидії.

Було запропоновано універсальний метод протидії атакам спеціального виду, які використовують CPA, DPA та SPA першого роду, який базується на рандомізації тимчасових даних *t* та рандомізації масиву b. Це дозволило ускладнити візуальний аналіз спектру енергоспоживання, та для винесення припущення порушнику буде потрібно зібрати сліди енергоспоживання n - операцій згортання.

Для більш точної та правильної оцінки складності реалізації атаки спеціального виду потрібно атаку поділити на етапи та мати на увазі наступні теоретичні відомості:

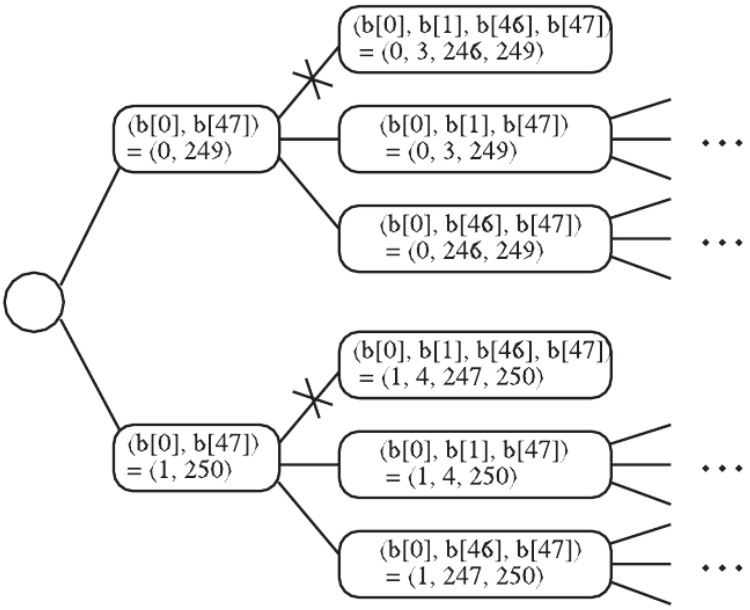

Рисунок 4 – Приклад дерева пошуку при B=[…,239,242,244,245,246,249

Теорема 1. Якщо функція D, яка корельована до непересічної множини k біт ключа і загальної L довжини ключа, де L/k – ціле число, то порушнику буде потрібно обчислити $2^k \bullet L/k$ слідів енергоспоживання для того, щоб дізнатися всі бітів ключа L (наприклад, алгоритм DES, $k=6$, $L=48$, тобто потрібно вивчити 512 слідів).

Теорема 2. В узагальненій d біт атаці на n-бітному процесорі, при парному n, середня частина сигналу енергоспоживання, яка придатна до аналізу, буде

$$\begin{cases} \left[2\sum_{k=d}^{n} \binom{n}{k} \right] / 2 & \text{if } d > n/2 \\ 1 & \text{if } 0 < d \le n/2 \end{cases}. \qquad (10)$$

Тобто при виборі d більше ніж $n/2$ буде виникати випадок, коли порушник буде отримувати або все, або нічого. Для цього потрібно встановити поріг-обмеження при виборі d, це збільшить кількість сигналів для дослідження, але зменшить імовірність некоректного припущення (див. рис. 5).

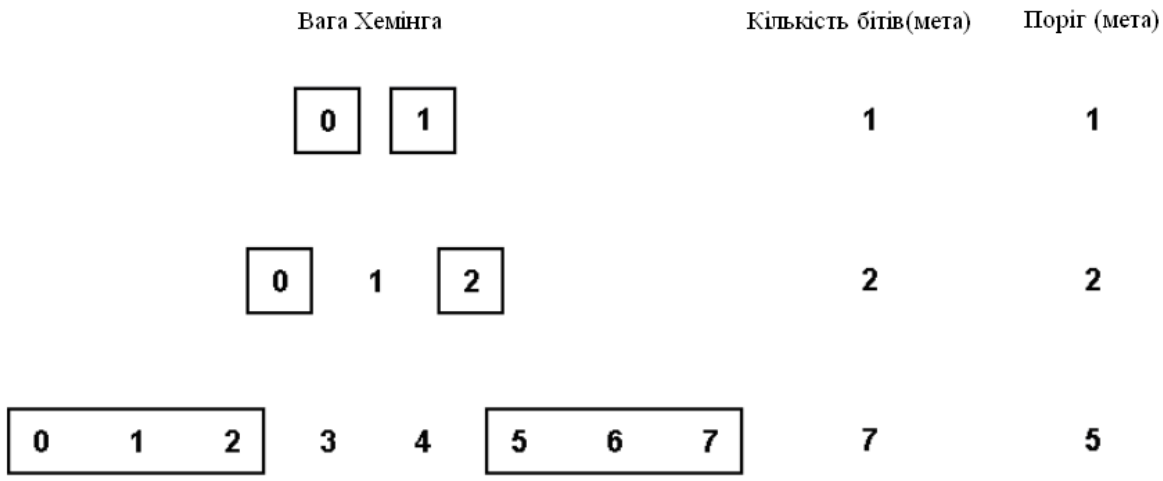

Рисунок 5 – Поріг для вибраної функції

Теорема 3. Щоб зберегти достатню умову співвідношення корисного сигнал/шум (SNR) «все-або-нічого» для d - бітної DPA атаки як і для деякого співвідношення корисного сигнал/шум 1-бітної DPA атаки, порушнику потрібно зробити, в середньому, $2^{d-1} / d^2$ сигналів енергоспоживання, таких самих як і при 1-бітній DPA атаці.

Отримані практичні результати сформувалися у вигляді таблиці 3.

Таблиця 3 – Порівняння методів протидії

Алгоритм згортання	ПЗП/ ROM	ОЗП/ RAM	Затрачений час	Складність, кількість операцій	Метод якому протидіє
Алгоритм 5.1 (без застосування протидії)	3796	1063	67.383	–	-
Рандомізація t	3980	1063	71.191	n	SPA
Засліплення с з цілим r	4022	1064	69.043	1	CPA
Засліплення с з багаточленом R(X)	4194	2067	101.953	1	CPA
Рандомізація b	4050	1063	70.117	1	CPA
Рандомізація t та рандомізація b	4106	1064	73.828	n	SPA, CPA

У **висновках** стисло викладено основні практичні результати, отримані у ході дисертаційних досліджень.

У **додатках** наведено акти впровадження отриманих результатів, акти впровадження та RTL-схеми макету програмно-апаратної реалізації деяких функції NTRU.

ВИСНОВКИ

Забезпечення конфіденційності, цілісності та автентичності даних, які передаються по незахищеним каналам зв’язку, є актуальною задачею, але складнішою задачею є забезпечення причетності одержувача даних. Вирішувати цю задачу можна за рахунок використання направлених шифрів. У зв’язку з цим актуальною задачею є обґрунтований вибір схеми НШ, тобто пошук такої схеми НШ яка відповідала б сучасним вимогам - високі швидкісні характеристики, стійкість до сучасних атак, враховуючи нові тенденції в сфері створення квантового комп’ютера.

Проведений аналіз дозволив визначити, що до основних методів НШ, що знайшли застосування, необхідно віднести: метод НШ в кільці (RSA-

перетворення); метод НШ в полі Галуа F(p); метод НШ в групі точок еліптичних кривих E(F(q)) та метод НШ на решітках.

Провівши порівняльний аналіз між RSA, ECC та NTRU з метою визначення кращої кандидатури на проект національного стандарту НШ в Україні, використовуючи при цьому метод визначення вагових коефіцієнтів на основі функції втрати ефективності систем, отримали наступні результати: формально NTRU має значну перевагу, приблизно у 6 разів, над RSA та ECC - у 7 разів.

Нині запропоновано ряд аналітичних криптоатак, що направлені на компрометацію особистих ключів. В процесі класифікації атак виявлено значне число аналітичних, в тому числі і атак спеціального виду. Їх аналіз підтвердив, що принципово можливі їх реалізації. При цьому важливим є завдання визначення найбільш ефективної з точки зору криптоаналітика атак, тобто атак з найменшою складністю.

Відносна легкість, менша обчислювальна складність реалізації атак спеціального виду робить їх суттєвою загрозою. Саме тому виникає задача дослідження програмно-апаратної реалізації алгоритму з метою пошуку можливих критичних вразливостей та недоліків реалізації, та в подальшому пошук механізмів уникнення або запобігання вразливостям.

На основі аналізу основних методів аналізу: SPA, DPA та CPA спектру енергоспоживання на програмно-апаратній реалізації криптосистеми NTRU, виявлено можливі вразливості, використовуючи які порушник зможе отримати додаткову інформацію про обчислення операцій згортки у пристрої та відповідно зробити спробу відновити конфіденційну інформацію.

Підтверджено, що існує можливість відновити особистий ключ за допомогою отримання додаткової інформації про процес обчислення криптографічних операцій, якщо порушник отримує дані про кількість звернень K до геш-функції. Перекриття цієї вразливості можна здійснити засобом дублювання звернень до геш-функції. Але у такій модифікованій версії NTRU кількість звернень до геш-функції збільшиться удвічі, що ускладнить реалізацію атаки за рахунок збільшення розміру таблиці можливих припущень. Запропоновано метод використання додаткових «додавань». Сутність метода полягає у визначенні максимального значення K_{max} кількості звернень до геш-функції і обчислені додаткових звернень $K_{max} - K$ у випадку, коли кількість звернень буде меншою ніж максимальне значення.. При цьому час виконання зашифрування буде збільшуватися, але несуттєво(на 9%).

Визначено якщо порушник отримує достатньо статистичних даних про операції згортки на деякій множині багаточленів, він, проаналізувавши енергоспоживання отриманих операцій згортки та використовуючи вирази $P(y \to z) \approx mHD(y,z) + n = mHW(y \oplus z) + n$ та $HW(x \oplus (x + y))$, може припустити, що можна знайти залежність зсувів при використанні рандомізованого вектору r_k. Далі відфільтрувавши рандомізований вектор r_k, як шум, порушник зможе провести атаку спеціального виду, задача якої буде відновлення особистого ключа.

На основі аналізу існуючих методик оцінки складності, було виявлено наступне: складність алгоритму (кількість простих елементів, які будуть впливати

на спектр енергоспоживання); кількість потрібних слідів енергоспоживання; вид атаки, що реалізується (d - бітна атака, де d – кількість бітів, що відстежується), розмір жорсткого диску – у сумі це надає оцінку складності реалізації атаки спеціального виду на енергоспоживання.

Визначено, що найбільш ефективним (у разі ускладнення реалізації атаки при найменшому впливі на первинні характеристики алгоритму) буде комбінований метод: рандомізація b та t одночасно. Перша рандомізація використовується з метою ускладнення SPA-атаки, інша – збільшить кількість потрібних статистичних даних, які потрібно буде отримати порушнику для визначення особистого ключа.

За результатами проведених теоретичних та експериментальних досліджень і розробок у дисертації досягнуті наступні теоретичні результати:

1) Розроблено універсальний метод протидії може бути використаний як метод протидії атакам спеціального виду на реалізацію, які базуються на аналізі спектру енергоспоживання, підвищивши стійкість у n-разів.

2) Вдосконалено метод направленого шифрування на решітках, ANSI X9.98 NTRU, підвищує стійкість до атак спеціального виду на реалізацію, які використовують SPA-метод, програючи у зростанні часу обчислення майже на 9%.

3) Вперше сформовано перелік вимог для схем направленого шифрування, який відрізняється від відомих тим, що враховує аспекти криптографічної стійкості за умови появи квантових комп'ютерів. На основі переліку вимог був проведений аналіз сучасних та перспективних схем НШ з метою виявлення кращої схеми НШ. Аналіз проводився за допомогою методу визначення вагових коефіцієнтів на основі функції втрати ефективності. Було визначено наступне: NTRU виграє у RSA у 6 разів, ECC у свою чергу поступається RSA – приблизно у 1,04 разів

4) Аналізуючи результати існуючих досліджень та отриманих практичних результатів, стало зрозуміло, що більшість атак на методи направленого шифрування на решітках або неефективні для існуючих потужностей (наприклад, атака грубої сили), або можуть бути усунені шляхом незначних модифікацій (удосконалення програмно-апаратної реалізації. Тому алгоритм ANSI X9.98 NTRU можна визнати проектом національного стандарту України.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Іваненко, Д.В. Проблемні питання електронної автентифікації в системах контролю доступу / Д.В. Іваненко, Є.П. Колованова // Прикладна радіоелектроніка. – 2010. - №3. - С. 401-403.

2. Балагура, Д.С. Основні аспекти захищеності механізмів автентифікації PIV-картки. / Д.С. Балагура, Д.В. Іваненко // Прикладна радіоелектроніка. Тематичний випуск, присвячений проблемам забезпечення безпеки інформації. - 2011. - С.255-258.

3. Бондаренко, М.Ф. Атака спеціального виду на NTRU / М.Ф.Бондаренко, Д.С. Балагура, Д.В. Іваненко // Прикладна радіоелектроніка. - 2012. - С. 105-108.

4. Іваненко, Д.В. Порівняльний аналіз сучасних асиметричних криптосистем / Д.В. Іваненко, О.В. Севєрінов // Системи управління, навігації та зв'язку. - 2012. – Вип. 2 (22). – С. 61-64.

5. Іваненко, Д.В. Класифікація атак спеціального виду на енергоспоживання / Д.В. Іваненко // Системи обробки інформації. – 2012. – Вип. 7 (105). – С.17- 22.

6. Іваненко, Д.В. Методи протидії атакам спеціального виду на крипто перетворення NTRU, які базуються на аналізі енергоспоживання / Д.В. Іваненко // Системи управління, навігації та зв'язку. – 2012.– Вип. 3(23). – С. 63-70.

7. Іваненко, Д.В. Аналіз механізмів и методів електронної ідентифікації та автентифікації в PIV системах / Д.В. Іваненко, П.А. Філоненко // РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»: тез. докл. 14-го Ювілейного Міжнародного молодіжного форуму. – Харків. - 2010. –С.54.

8. Іваненко, Д.В. Проблемні питання електронної автентифікації в системах контролю доступом / Д.В. Іваненко, Є.П. Колованова // Комп'ютерне моделювання в наукомістких технологіях: тез. докл. науково-технічної конференції з міжнародною участю. – Харків. - 2010. –С.148-151.

9. Іваненко, Д.В. Обгрунтування вимог до ідентифікації обєктів в системах електронної цифрового підпису в Україні / Д.В. Іваненко, П.А. Філоненко, Є.П. Колованова // Безпека інформації в інформаційно-телекомунікаційних системах: тез. докл. XIII Міжнародної науково-практичної конференції. – Київ. - 2010. – С.35-36.

10. Іваненко, Д.В. Методи та мехнізми автентифікації на основі електронних засобів типу PIV картка / Д.В. Іваненко, П.А. Філоненко // Безпека інформації в інформаційно-телекомунікаційних системах: тез. докл. XIII Міжнародної науково-практичної конференції. – Київ. - 2010. – С.108.

11. Іваненко, Д.В. Перспективні використання біометричних методів в сучасних ІВК / Д.В. Іваненко, П.А. Філоненко // CSV-2010: тез. докл. IV міжнародної конференції молодих вчених. - Львів. – 2010. –С.342-344.

12. Іваненко, Д.В.Применение биометрических систем с использованием интеллектуальных методов защиты информации в банковской сфере / Д.В. Іваненко, П.А. Філоненко // Наукові дослідження молоді — вирішенню проблем європейської інтеграції: тез. докл. VI Всеукраїнської студентської науково-практичної конференції. – Харків. – 2011. – CD. - 3с.

13. Іваненко, Д.В. Анализ биометрических систем защиты информации от НСД с использованием интеллектуальных методов / Д.В. Іваненко, П.А. Філоненко // Радіоелектроніка та молодь у xxi столітті: тез. докл. 15-го Ювілейного Міжнародного молодіжного форуму. –Харків. – 2011. – С.233-245.

14. Бондаренко, М.Ф. Атака по времени на NTRU/ М.Ф. Бондаренко, Д.С.Балагура, Д.В.Іваненко // Комп'ютерне моделювання в наукомістких технологіях: тез. докл. науково-технічної конференції з міжнародною участю. –Харків. - 2012. – CD. -1с.

15. Бондаренко, М.Ф.Атака специального вида на NTRU / М.Ф. Бондаренко, Д.С.Балагура, Д.В.Іваненко // Безпека інформації в інформаційно-телекомунікаційних системах: тез. докл. XV Міжнародної науково-практичної конференції. – Київ. - 2012. – С.110.

16. Іваненко, Д.В. Класифікація атак спеціального виду на енергоспоживання» / Д.В. Іваненко // «Інфокомунікації – сучасність та майбутнє: тез. докл. Другої міжнародної науково-практичної конференції молодих вчених. – Одеса. - 2012– С.8-9.

АНОТАЦІЯ

Іваненко Д.В. Методи підвищення стійкості схем направленого шифрування в кільцях зрізаних поліномів до атак спеціального виду на реалізацію.– На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Харківський національний університет радіоелектроніки МОН України, Харків, 2013.

Дисертаційна робота присвячена дослідженню та обґрунтуванню вибору методу направленого шифрування на решітках, ANSI X9.98 NTRU, національним стандартом України.

Запропоновано вдосконалений метод направленого шифрування на решітках, ANSI X9.98 NTRU, що на відміну від існуючих дозволяє забезпечити стійкість до атак спеціального виду на реалізацію, які використовують SPA-метод, за рахунок використання додаткових «додавань» внаслідок чого на, приблизно, 9% зросте час обчислення алгоритму.

Запропоновано універсальний метод протидії атакам спеціального виду, яку базуються на аналізі спектру енергоспоживання, який на відміну від відомих ґрунтується на рандомізації t та рандомізації масиву b, що дозволяє підвищити стійкість алгоритму NTRU у n - разів.

Ключові слова: теорія решіток, багаточлен, атака спеціального виду, енергоспоживання, SPA, DPA, CPA, метод Хемінга, відстань Хемінга, операція згортки.

АННОТАЦИЯ

Иваненко Д.В, Методы повышения стойкости схемы направленного шифрования в кольцах срезанных полиномов к атакам специального вида на реализацию. – На правах рукописи.

Диссертация на соискание учёной степени кандидата технических наук по специальности 05.13.21 – системы защиты информации. – Харьковский национальный университет радиоэлектроники МОН Украины, Харьков, 2013.

Диссертация посвящена исследованию обоснованию выбора схемы направленного шифрования в кольцах срезанных полиномов, ANSI X9.98 NTRU, национального стандарта Украины.

Предложено усовершенствованный метод схемы направленного шифрования в кольцах срезанных полиномов, ANSI X9.98 NTRU, что в отличии от существующих позволяет обеспечить стойкость до атак специального вида на

реализацию, которые используют SPA – метод, за счет использования дополнительных «дополнений» в результате чего на, близко, 9% вырастит время вычисления алгоритма.

Предложен универсальный метод противодействия атакам специального вида, который основывается на рандомизации t и рандомизации массива b, что позволяет повысить стойкость алгоритма NTRU в n – раз.

Ключевые слова: теория решеток, атака специального вида, SPA, DPA, CPA, метод Хемминга, расстояние Хемминга, энергопотребление, полином.

ABSTRACT

Ivanenko D.V. Survivability improving methods for directional encryption schemes over truncated polynomials rings against side channel attacks on the implementation. – The manuscript.

Thesis for a Ph.D. science degree by specialty 05.13.21 – information security systems. – Kharkiv National University of Radioelectronics of the MES of Ukraine, Kharkiv, 2013

The thesis is devoted to research and justification of directional encryption schemes over truncated polynomials rings, ANSI X9.98 NTRU, that in contrast to the existing approaches allows to reach resistibility against side channel attacks on the implementation using SPA method that is based on operating with additional components, it results in 9% growth of the algorithm calculations time.

There is a new universal reaction method against side channel attacks is proposed in the thesis, it is based on randomization of the t parameter and the b array that allows to increase the NTRU algorithm strength by n times.

Keywords: Lattice, side channel attacks, SPA, DPA, CPA Hamming distance, Hamming weight, consumption energy, the polynomial.