# Проблема стандартизації криптографічних перетворень в перехідний та постквантовий періоди та стан її вирішення

І. Д. Горбенко[1,2], О. Г. Качко[2],
Ю. І. Горбенко[2], М. В. Єсіна[1,2],
В. А. Пономар[2]

1. Кафедра безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, Україна, Харків, пл. Свободи, 6, E-mail: gorbenkoi@iit.kharkov.ua, m.v.yesina@karazin.ua

2. АТ «Інститут інформаційних технологій», Україна, Харків, вул. Бакуліна, 12, E-mail: iit@iit.kharkov.ua, gorbenkou@iit.kharkov.ua, Laedaa@gmail.com

***Коротка анотація – Розглядаються та аналізуються загрози, що мають бути реалізовані у постквантовий період стосовно існуючих стандартів криптографічних перетворень. Обґрунтовуються вимоги до них. Формулюється проблема розробки, стандартизації та застосування постквантових стандартів, наводиться аналіз стану та визначаються шляхи її вирішення.***

Ключові слова – вимоги до постквантових перетворень, криптографічна стійкість та складність, перспективні методи асиметричних перетворень, стан розробки стандартів та їх порівняння, шляхи впровадження.

## I. Вступ

Нині, та очевидно, в деякій перспективі, для криптографічного захисту інформації застосовуються та будуть застосовуватись методи та алгоритми криптоперетворень, що орієнтовані на застосування існуючих, стандартизованих. Вони є суттєвою складовою забезпечення кібербезпеки. Але є обґрунтовані підозри, що у постквантовий період існуючі стандарти асиметричних криптоперетворень, будуть зламуватись за допомогою квантових криптоаналітичних систем криптоаналітиком 3-го рівня з поліноміальною чи суб'експоненційною складністю. Важливою особливістю постквантового періоду є значна невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів (КВК), їх математичного та програмного забезпечень, а також застосування для криптоаналізу існуючих криптоперетворень та криптопротоколів [1, 2]. Їх застосування необхідно розглядати щодо перехідного та постквантових періодів. Перехідний період пропонується визначити як проміжок часу у майбутньому, коли будуть суттєво вдосконалені класичні методи та засоби криптоаналізу, а також будуть створені та застосовуватись для криптоаналізу квантові комп'ютери з обмеженими потужностями. У цей період, можуть бути застосованими деякі існуючі нині стандарти асиметричних та симетричних криптографічних перетворень, але з максимально можливими чи збільшеними довжинами та властивостями загальносистемних параметрів та ключових даних, в тому числі при використанні в системі Блокчейн (БЧ). Постквантовий період пропонується визначити як проміжок часу у майбутньому, коли будуть суттєво удосконалені класичні методи та створені КВК з необхідними для успішного криптоаналізу довжинами регістрів (в кубітах) та необхідне для їх реалізації математичне та програмне забезпечення, особливо при сумісному застосуванні ІТ сумісно з БЧ.

Нині уже практично створені та застосовуються квантові комп'ютери. Стан створення та можливості застосування КВК є такими [1, 2]:

- IBM повідомила про план запуску в жовтні 2019 53 кубітного КВК;
- 53 – кубітний КВК IBM має нову конструкцію процесора, масштабуємий, знижена ймовірність помилок, надійний в хмарі;
- IBM відкриває новий обчислювальний центр в Нью-Йорку, 1 – 53 кубіт, 5 – 20 кубіт (14 в перспективі);
- 72 кубітний КВК Google за 3.5 хвилини виконує еквівалент роботи 10 тис. р. найпотужного кластера.

Стан створення асиметричних криптоперетворень типу електронний підпис (ЕП), асиметричний шифр (АСШ) та протокол інкапсуляції ключів (ПІК) наведено нижче [1, 2]:

- 2006 – 1ша PQC конференція у Льовен, Бельгія;
- 2009 – Дослідження NIST PQC Квантовостійка криптографія з відкритим ключем: опитування [Perlner, Cooper];
- 2012 – NIST починає проект PQC;
- Квітень 2015 – Семінар NIST з питань кібербезпеки в постквантовому світі;
- Серпень 2015 – Оголошення АНБ;
- Лютий 2016 – Звіт NIST про PQC (NISTIR 8105);
- Лютий 2016 – Оголошення NIST про "змагальний процес" у PQCrypto в Японії;
- Грудень 2016 – Опубліковані підсумкові вимоги та критерії оцінювання;
- Листопад 2017 – Кінцевий термін подання заявок;
- Грудень 2017 – Початок першого туру – 69 кандидатів, прийнято як "повні та вірні";
- Квітень 2018 – 1й семінар зі стандартизації NIST PQC;
- Січень 2019 – оголошено кандидатів 2 раунду;
- Серпень 2019 – 2й семінар зі стандартизації NIST PQC.

NIST США для оцінювання існуючих та перспективних проектів стандарту щодо ЕП, АСШ та ПІК запропоновані та уже використовуються такі рівні безпеки:

- I Рівень Принаймні так важко зламати, як AES128 (вичерпний перебір ключів);
- II Рівень Принаймні так важко зламати, як SHA256 (пошук колізії);
- III Рівень Принаймні так важко зламати, як AES192 (вичерпний перебір ключів);
- IV Рівень Принаймні так важко зламати, як SHA384 (пошук колізії);
- V Рівень Принаймні важко зламати, як AES256 (вичерпний перебір ключів).

NIST попросив заявників зосередитись на рівнях 1, 2 та 3 (рівні 4 і 5 призначені для дуже високої безпеки).

Продуктивність – вимірюється на різних класичних платформах.

Інші властивості: Змінні дані (параметри), ідеальна пряма секретність, простота та гнучкість, зловживання стійкістю та ін. стійкість до атак бічними каналами**.**

Метою доповіді є аналіз стану захищеності існуючих криптографічних перетворень та обґрунтування необхідності, стану розробки, дослідження та прийняття постквантових стандартів криптоперетворень, розгляд існуючої проблеми постквантової стандартизації та шляхів її вирішення на міжнародному та національному рівнях.

## II. Сутність та стан вирішення проблеми постквантової криптографії на світовому рівні

NIST США провів 1-й етап конкуру щодо кандидатів на стандарти постквантових асиметричних криптографічних примітивів. Із 64 кандидатів першого етапу до другого рекомендовано 26. Суттєві досягнення зі створення математичних та програмних моделей перетворень на квантових комп'ютерах за оцінками провідних світових фахівців в галузі кібербезпеки, призвели до істотного прогресу в області криптографічного аналізу сучасних стандартизованих, особливо у постквантовий період. Вони зумовили стрімкий розвиток систем криптоаналізу.

Кандидатами на постквантові стандарти є симетричні шифри (СШ), АСШ (E2EE), ЕП та ПІК наведені нижче [1, 2]:

- симетричні блокові та потокові криптографічні перетворення (ДСТУ 7624:2014);
- криптографічні перетворення, що засновані на застосуванні геш-функцій (ДСТУ 7564:2014);
- асиметричні криптографічні перетворення на алгебраїчних решітках;
- криптографія, що заснована на кодах;
- криптографія, що заснована на складності обчислень ізогеній ЕК;
- багатовимірні криптоперетворення (мультиваріативні).

Основні вимоги до кандидатів на стандарти постквантових криптоперетворень можна конкретизувати у трьох таких напрямках:

- вимоги з безпеки (вимоги до стійкості до криптографічного аналізу);
- техніко-економічні вимоги (в основному щодо часової та просторової складностей);
- технічні характеристики реалізації алгоритмів асиметричних криптоперетворень.

Вимоги до стійкості мають бути сформульовані у відповідності до таких моделей загроз [1, 2]:

- для асиметричного шифрування – в умовах дії моделі IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack) – стійкість до атаки на основі адаптивно підібраного (вибраного) шифртексту;
- для електронного підпису – в умовах дії моделі EUF-CMA (Existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенційної підробки при атаках на основі адаптивно підібраного (вибраного) шифртексту;
- для протоколу обміну(встановлення, інкапсуляції) ключів – в умовах дії моделі безпеки Canetti-Krawczyk (СК-безпека).

Підсумки конкурсу за 1-й етап наведені в табл. 1. У ході виконання 1-го етапу в якості асиметричних постквантових механізмів рекомендовані механізми на основі: алгебраїчних решіток; математичних кодів (СВ-криптографія); мультиваріативного квадратичного перетворення; геш-функцій та ізогеній ЕК. Відповідні дані наведено в табл. 1 [1, 2].

ТАБЛИЦЯ 1

Підсумки 1-го етапу конкурсу

| | | | |
|---|---|---|---|
| На основі решіток | 5 | 21 | 26 |
| На основі кодів | 2 | 17 | 19 |
| На основі мультиваріативних перетворень | 7 | 2 | 9 |
| На симетричній основі | 3 | | 3 |
| Інші | 2 | 5 | 7 |
| Всього | 19 | 45 | 64 |

У таблиці 2 наведено проміжні результати, що отримані в ході початкових досліджень на 2-му етапі

ТАБЛИЦЯ 2

Підсумки 2-го етапу конкурсу

| | | | |
|---|---|---|---|
| На основі решіток | 3 | 9 | 12 |
| На основі кодів | 0 | 7 | 7 |
| На основі мультиваріативних перетворень | 4 | 0 | 4 |
| На симетричній основі | 2 | | 2 |
| Інші | 0 | 1 | 1 |
| Всього | 9 | 17 | 26 |

## III. Аналіз стійкості існуючих кандидатів на постквантові стандарти

До основних задач, які можуть бути вирішені на квантовому комп'ютерові необхідно віднести такі [1]:

1) квантовий алгоритм факторизації Шора;
2) квантовий алгоритм Гровера пошуку елемента в несортованій базі;
3) квантовий алгоритм Шора для розв'язку дискретного логарифму в скінченому полі;
4) квантовий алгоритм розв'язку дискретного логарифму в групі точок ЕС Шора;
5) квантові алгоритми криптоаналізу для перетворень в фактор кільці;
6) квантовий алгоритм криптоаналізу Ксіонга та Ванга та його вдосконалення тощо.

Основними критеріями обмеження квантових атак є:

- $2^{40}$ логічних вентилів, тобто приблизної кількості вентилів, яка буде послідовно виконуватись за рік;
- $2^{64}$ логічних вентилів, яку сучасні класичні обчислювальні архітектури можуть виконувати послідовно за десять років;
- не більше, ніж $2^{96}$ логічних вентилів, тобто приблизна кількість вентилів як кубіти атомного масштабу зі швидкістю світла часу поширення може виконувати за тисячоліття.

Криптографічна стійкість перспективних проектів повинна бути такою:

1) Стійкість проти класичних атак – Класична безпека.

2) Стійкість проти «квантових» атак. Зокрема, стійкість до алгоритму Гровера (необхідність подвоєння розміру ключа) – Квантова безпека.

3) Базування на задачах, які мають високу складність обчислення. Можливе ігнорування зниження рівня складності, за умови, що практична стійкість не зміниться – Доказова безпека.

4) Можливість використання у протоколах типу TLS 1.3 з підтримкою forward secure cipher suites – Довгострокова безпека.

5) Стійкість проти атак з адаптивним підбором – Активна безпека.

Повинна бути забезпеченою стійкість проти атак спеціального виду. Реалізація цих атак направлена на пошук вразливостей у практичній реалізації криптосистеми, в першу чергу засобу КЗІ:

- контроль над обчислювальним процесом;
- спосіб доступу до системи чи засобу;
- метод безпосереднього здійснення атаки тощо.

В основу захисту від атак спеціального виду можуть бути покладеніособливості:

- фіксована кількість звернень до геш-функції;
- рандомізація даних;
- незалежність ключів від значень тощо.

Результати порівняльного аналізу складності факторизації для класичного та квантового алгоритмів наведені в таблиці 3.

ТАБЛИЦЯ 3

Результати порівняльного аналізу складності факторизації

| Розмір модуля N, бітів | Кількість необхідний кубітів, $2n$ | Складність квантового алгоритму, $4n^3$ | Складність класичного алгоритму |
|---|---|---|---|
| 512 | 1024 | $0{,}54\cdot10^{9}$ | $1{,}6\cdot10^{19}$ |
| 3072 | 6144 | $12\cdot10^{10}$ | $5\cdot10^{41}$ |
| 15360 | 30720 | $1{,}5\cdot10^{13}$ | $9{,}2\cdot10^{80}$ |

Результати порівняльного аналізу складності дискретного логарифмування для класичного та квантового алгоритмів наведені в таблиці 4.

ТАБЛИЦЯ 4

Результати порівняльного аналізу складності дискретного логарифмування

| Алгоритм розв'язку дискретного логарифмічного рівняння | | | |
|---|---|---|---|
| Розмір порядку базової точки, бітів | Кількість необхідний кубітів $f(n)=7n+4\log_2 n+10$ | Складність квантового алгоритму $360n^3$ | Складність класичного алгоритму |
| 163 | 1210 | $1{,}6\cdot10^{9}$ | $3{,}4\cdot10^{24}$ |
| 256 | 1834 | $6\cdot10^{9}$ | $3{,}4\cdot10^{38}$ |
| 571 | 4016 | $6{,}7\cdot10^{10}$ | $8{,}8\cdot10^{85}$ |
| 1024 | 7218 | $3{,}8\cdot10^{11}$ | $1{,}3\cdot10^{154}$ |

Основними завданнями 2-го етапу є такі (NIST ще відкритий для злиття заявлених проектів):

- Нові оператори IP потрібні тільки в разі приєднання нових членів команди або зміни статусу IP;
- Згодом питання, пов'язані з IP, можуть зіграти більшу роль у прийнятті наших рішень;
- 2-й раунд триватиме 12-18 місяців, після чого ми очікуємо, що відбудеться 3-й раунд;
- Загальна хронологія: NIST ще очікує проекти стандартів близько 2022 року (але залишає за собою право змінити це!).

## IV. Стан створення постквантових стандартів на національному та міжнародному рівнях

В Україні розроблені та рекомендовані до застосування постквантові стандарти таких симетричних криптоперетворень.

1. Алгоритм блокового симетричного перетворення ДСТУ 7624:2014 – 10 режимів роботи (128, 256, 512біт) (5-7 рів.).

2. Функція гешування ДСТУ 7564:2014 (8–512 біт) (5-7 рів.).

3. Алгоритм симетричного потокового перетворення ДСТУ 8845:2019 (256–512 біт) (5-7 рівень).

4. На стадії розгляду першої редакції знаходиться проект стандарту «Алгоритми асиметричного шифрування та інкапсуляції ключів» (алгебраїчні решітки, стійкість 256, 384, 512 біт).

5. Розроблено проект та на стадії досліджень знаходиться проект стандарту «Електронний підпис» (алгебраїчні решітки, стійкість 256, 384, 512 біт).

Постквантові кандидати на ЕП за 2-й етап наведено в таблиці 5 [1, 2].

ТАБЛИЦЯ 5

Постквантові кандидати на ЕП за 2-й етап

| Математичні методи ЦП | Кандидати в стандарти ЦП | Число |
|---|---|---|
| Алгебраїчні решітки | Crystals-Dilithium, Falcon, qTesla | 3 |
| Геш-перетворення | Sphincs+ | 1 |
| Кінцеві автомати | Picnic | 1 |
| Мультиваріативні перетворення | Gemss, Luov, Mqdss, Rainbow | 4 |
| Усього | | 9 |

Механізми постквантових кандидатів на АСШ та ПІК за 2-й етап наведено в таблиці 6 [1, 2].

ТАБЛИЦЯ 6

Постквантові кандидати на АСШ та ПІК за 2-й етап

| Математичні методи ПІК | Кандидати в стандарти ПІК | Число |
|---|---|---|
| Алгебраїчні коди | BIKE, Classic McEliece, HQC, LEDAcrypt (LEDAkem, LEDApkc), NTS-KEM, Rollo (Locker, Ouroboros-r(lattice)), RQC | 7 |
| Алгебраїчні решітки | Crystals-Kyber, FrodoKEM, LAC, NewHope, NTRU (NTRUEncrypt, NTRU-HRSS-KEM), NTRU Prime, Round5 (Hila5, Round2), Saber, Three bears | 9 |
| Інші перетворення | SIKE (ізогенії) | 1 |
| Усього кандидатів | | 17 |

## V. Сутність методу асиметричного шифрування та інкапсуляції ключів

В якості основного математичного методу постквантового АСШ та ПІК вибрано NTRU-подібні криптоперетворення. Нині вони отримали назву як таких, що ґрунтуються на алгебраїчних решітках. Вказана назва пов'язана з тим, що доведення їх криптографічної стійкості зводиться до застосування математичного апарату алгебраїчних решіток, а також, по суті, NTRU криптографічне перетворення є безпосередньо алгебраїчною решіткою.

Проведені дослідження підтвердили можливість використання цих параметрів для шифрування з боку дуже важливої характеристики – швидкодії.

Зважаючи на національні вимоги, можливості та реалізацію національного стандарту симетричного шифрування ДСТУ 7624-2014, стосовно проекту національного АСШ висунуто вимоги, що будь-яка атака, що порушує певне визначення безпеки застосування АСШ, повинна вимагати обчислювальні ресурси порівняні з, або більші, ніж необхідні для пошуку 512-бітного ключа (наприклад, Калина-512) стосовно класичної атаки та 256-бітного ключа стосовно квантової атаки.

Додатковими властивостями щодо криптографічної стійкості АСШ є наступні.

Повна пряма захищеність. Цей термін вживається для позначення характеристик ключа у протоколах узгодження, який надає гарантії, що попередній сеансовий ключ не буде скомпрометований, якщо навіть секретний ключ серверу був скомпрометований. Хоча ця властивість виконується при стандартному шифруванні, вартість такої операції може бути недозволеною в деяких випадках.

Ще одним випадком взаємовпливу захищеності та швидкодії є здатність протидії атакам по стороннім каналам. Більш бажаними є схеми, що здатні протидіяти цим атакам при мінімальній вартості.

Третьою бажаною властивістю є протидія мультиключовим атакам. В ідеалі атакуючий не повинен відчувати різницю, коли його мета – скомпрометувати одну пару ключів або велику кількість пар ключів.

Остання вимога, недостатньо добре визначена, – це стійкість до неправильного використання механізму АСШ. Бажано щоби АСШ не міг ставати непрацездатними через окремі помилки в коді, несправності у генераторі випадкових чисел.

Остання вимога, недостатньо добре визначена, – це стійкість до неправильного використання механізму АСШ. Бажано щоби АСШ не міг ставати непрацездатними через окремі помилки в коді, несправності у генераторі випадкових чисел.

У таблиці 7 наведені ідентифікатори та характеристики механізмів (алгоритмів) АСШ, що обрані для їх порівняння, при чому швидкодія $T_{пр.}$ та $T_{зв.}$ задана в мільйонах ($10^6$) тактів [1] роботи комп'ютера.

При дослідженні з метою вибору кращих алгоритмів також були висунуті додаткові безумовні вимоги [3]:

1) алгоритм повинен гарантувати, щонайменше 5 рівень безпеки за класифікацією NIST;

ТАБЛИЦЯ 7

Характеристики алгоритмів шифрування

| Алгоритми | Тип | $I_{ст.}$ | $l_{в.к}$ | $l_{о.к}$ | $l_{рез.}$ | $T_{пр.}$ | $T_{зв.}$ |
|---|---|---|---|---|---|---|---|
| Giophantus | Lattices | 5 | 27204 | 1134 | 54408 | 420,543208 | 792,577 |
| KINDI | Lattices | 5 | 2368 | 2752 | 3328 | 0,705 | 0,919 |
| LAC | Lattices | 5 | 1056 | 2080 | 2048 | 0,137258 | 0,133 |
| LEDApkc | Codes | 5 | 12384 | 40 | 24768 | 92,84 | 264,938 |
| LIMA | Lattices | 5 | 12289 | 18433 | 12291 | 0,909 | 1,126 |
| Lizard | Lattices | 5 | 8192 | 998266 | 8512 | 0,805 | 0,568 |
| LOTUS | Lattices | 5 | 1470976 | 1630720 | 1768 | 0,901 | 1,087 |
| McNie | Codes | 5 | 630 | 584 | 729 | 3,504 | 7,707 |
| NTRUEncrypt | Lattices | 5 | 64232 | 63912 | 127696 | 174,2 | 0,299 |
| Odd Manhattan | Lattices | 5 | 4454241 | 4456650 | 616704 | 141,625 | 155,302 |
| OKCN/AKCN/CNKE | Lattices | 5 | 1312 | 992 | 1200 | 0,568 | 0,631 |
| Round2 | Lattices | 5 | 830 | 1039 | 953 | 0,905 | 1,135 |
| RQC | Codes | 5 | 40 | 1795 | 3574 | 6,46 | 18 |
| Titanium | Lattices | 5 | 23552 | 32 | 8320 | 2,974 | 0,561 |
| NTRU Prime Ukraine | Lattices | 5 | 1578 | 243 | 1578 | 0,074 | 0,138 |

2) якщо існує декілька варіантів наборів параметрів для одного алгоритму, то в порівнянні бере участь варіант, що гарантує найбільшу безпеку.

3) Перспективний проект стандарту АСШ повинен також, при необхідності, забезпечувати 512 бітну класичну криптографічну стійкість та відповідно 256 бітну квантову криптографічну стійкість.

На рис. 1 відображено гістограму відносної переваги алгоритмів. Як видно найбільшу перевагу має алгоритм NTRU Prime Ukraine, на другому місці – LAC, на третьому – OKCN/AKCN/CNKE.

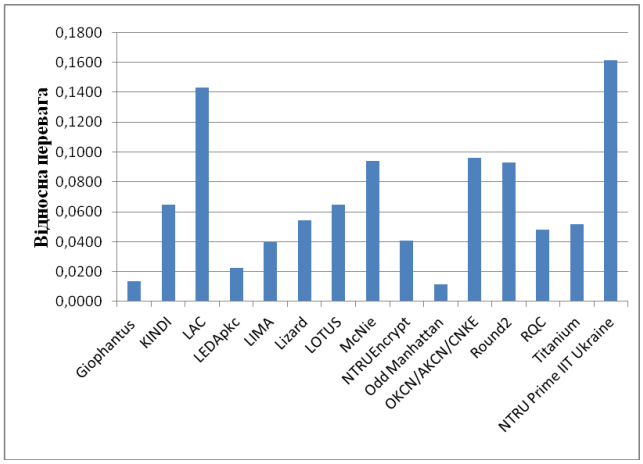


Рисунок 1 – Відносна перевага алгоритмів шифрування

## VI. Основні властивості національного постквантового стандарту (перша редакція) «Скеля»

У даному розділі наведено основні характеристики та властивості національного постквантового стандарту «Скеля» [4].

У таблиці 8 наведено основні загальні параметри АСШ «Скеля».

У таблиці 9 наведено основні параметри для генерації ключа «Скеля».

ТАБЛИЦЯ 8

Основні загальні параметри АСШ «Скеля»

| Позн. | Призначення | Формула |
|---|---|---|
| $(Z/q)[x]$ | Кільце поліномів Кожен елемент $Z/q$ зазвичай кодується у $\lceil \log_2 q \rceil$ біт | |
| $n$ | Порядок поліному. Визначає кількість його коефіцієнтів. Просте число, для якого поліном $x^n - x - 1$ є незвідним | $n \geq \max\{3, 2t\}$ |
| $R$ | Поле поліномів $Z[x]$ з модулем $x^n - x - 1$ | $Z[x]/(x^n - x - 1)$ |
| $R/3$ | Поле поліномів $(Z/3)[x]$ з модулем $x^n - x - 1$ | $(Z/3)[x]/(x^n - x - 1)$ |
| $R/q$ | Поле поліномів $(Z/q)[x]$ з модулем $x^n - x - 1$ | $(Z/q)[x]/(x^n - x - 1)$ |
| $p$ | Менший модуль | $p = 3$ |
| $q$ | Більший модуль, просте число, за яким зводяться усі коефіцієнти поліному $R/q$ | $q \geq 48t + 3$ |
| $t$ | Натуральне число, кількість ненульових елементів поліному залежить від цього параметру. | $t \geq 1$ |
| $k$ | Рівень криптостійкості | 128, 256, 512 |
| $m$ | Таємне повідомлення. Кількість 0, 1 та -1 не менше, ніж $t$. | $m \in R/3$ |
| $M$ | Повідомлення після доповнення випадкового рядка $b$ та іншої інформації. | |
| *octL* | Поле для завдання довжини повідомлення | 1 байт |
| $e$ | Зашифроване повідомлення | $e \in R/q$ |

ТАБЛИЦЯ 9

Основні параметри для генерації ключа «Скеля»

| Позн. | Призначення | Формула |
|---|---|---|
| $G$ | Випадковий $t$-малий елемент (поліном), оборотний у $R/3$. Кількість ненульових елементів дорівнює 2n/3+1 Секретний параметр, що використовується для обчислення відкритого ключа. | $g \in R/3$ |
| $F$ | Випадковий $t$-малий елемент (поліном). Кількість ненульових елементів дорівнює 2t. Секретний параметр, що використовується для обчислення відкритого ключа. | |
| $f$ | Малий елемент (поліном), незвідний в $R/q$, є секретним (особистим) ключем. $f=p*F+1$ | $f = (1+3F) \bmod q$ $f \in R/q$ |
| $h$ | Відкритий ключ відправника. Оборотний елемент у $R/q$. | $h = p * G/f$ |
| $\underline{h}$ | $h$ перетворене в рядок октетів. Довжина $\underline{h}$ дорівнює $n\lceil \log_2 q \rceil$ | |

У таблиці 10 наведено додаткові параметри АСШ «Скеля».

ТАБЛИЦЯ 10

Додаткові параметри NTRUPrime Ukraine «Скеля»

| Позн. | Призначення | Формула |
|---|---|---|
| *qBits* | Кількість біт $q$ | $qBits = \lceil \log_2 q \rceil$ |
| $r$ | Засліплюючий поліном, випадковий $t$-малий елемент. | $r \in R/3$ |
| $b$ | Випадковий компонент (salt), що доповнює повідомлення. | |
| $db$ | Довжина випадкового компонента в бітах. Визначається рівнем криптостійкості. | $db = \begin{cases} 256 & k \leq 256 \\ 512 & k \leq 512 \end{cases}$ $db \bmod 8 \equiv 0$ |
| *Buffer Len Bits* | Довжина бітового рядка для його перетворення в малий поліном. Використовується при зашифруванні | $\lfloor (((n-1)/2) \cdot 3)/8 \rfloor \cdot 8$ |
| *maxMsgLenBytes* | Максимальна довжина повідомлення для зашифрування. | *bufferLenBits/8 – hLenBytes - 1* |
| $c$ | Кількість бітів, яка використовується для визначення індексу ненульового елементу полінома | $c_1 = \lfloor log_2 n \rfloor$; $c_2=c_1+1$ $c_3=c_2+1$; $c=c_i+1$ для якого $c_i \bmod n$ мінімально |
| *Llen* | Кількість байтів для завдання довжини повідомлення, що шифрується | $\log_{256}$ maxMsgLenBytes |
| *tm* | Кількість 1(-1) в поліномі, який створюється після перетворення повідомлення, що шифрується | *tm=t* |
| *Hash* | Геш-функція, що використовується | Залежить від криптостійкості |
| *Hlen* | Довжина геш-значення | *Hlen=k* |
| Min CallsR | Мінімальна кількість викликів функції гешування для створення полінома для осліплення | $\lceil t \cdot c / hashLenBits \rceil$ |

| | | |
|---|---|---|
| Min Calls Mask | Мінімальна кількість викликів функції гешування для маскування повідомлення | $\lceil \lceil n/5 \rceil \cdot 1.5 / hLenBits \rceil$ |
| pkLen | Кількість бітів відкритого ключа, які використовуються при формуванні рядка для шифрування | pkLen=db |
| OID | Ідентифікатор методу. 3 байти | $OID[0]=0; OID[1]=1; OID[2]=2;$ |

У таблиці 11 наведено часові характеристики функцій зашифрування та розшифрування АСШ «Скеля».

ТАБЛИЦЯ 11

Часові характеристики функцій зашифрування та розшифрування

| N | q | Encrypt | | | Decrypt | | | Decrypt | |
|---|---|---|---|---|---|---|---|---|---|
| | | Hash | Salsa20 | Snow20 | Hash | Salsa20 | Snow20 | Decrypt | Check |
| 439 | 6833 | 56908 | 40832 | 36308 | 81356 | 64280 | 60016 | 31708 | 29848 |
| 457 | 6037 | 64012 | 38200 | 34384 | 87948 | 61448 | 56868 | 30500 | 28496 |
| 461 | 7607 | 70592 | 42080 | 37724 | 99140 | 68572 | 63420 | 32524 | 32476 |
| 461 | 8779 | 70396 | 41964 | 37724 | 98352 | 68100 | 63220 | 32648 | 31928 |
| 467 | 3911 | 52828 | 32080 | 29592 | 72760 | 51528 | 48532 | 26908 | 23320 |
| 463 | 6529 | 65364 | 39124 | 35764 | 90484 | 63256 | 59072 | 32352 | 29220 |
| 463 | 6841 | 67780 | 40628 | 36500 | 94884 | 66448 | 61464 | 32336 | 30884 |
| 463 | 9371 | 70832 | 42824 | 38316 | 97344 | 68056 | 62296 | 33644 | 32756 |
| 479 | 5689 | 63824 | 38432 | 34144 | 87748 | 61556 | 57320 | 31000 | 28360 |
| 479 | 6089 | 65548 | 39072 | 35440 | 90624 | 62596 | 58352 | 32168 | 28948 |
| 491 | 6287 | 69464 | 41572 | 36188 | 94220 | 65984 | 61500 | 31368 | 30600 |
| 761 | 4591 | 74584 | 43640 | 41616 | 102232 | 71004 | 68984 | 40536 | 31820 |

У таблиці 12 наведено обчислювальну складність АСШ «Скеля».

ТАБЛИЦЯ 12

Обчислювальна складність АСШ «Скеля»

| Режим АСШ (Скеля) | Скеля 512 (SHA 256) Мбіт/с | Скеля 256 (SHA 256) Мбіт/с |
|---|---|---|
| Encrypt | 43 | 47 |
| Decrypt | 23 | 29 |
| Режим АСШ (Скеля) | Скеля 512 (Купина 512) Мбіт | Скеля 256 (Купина 256) Мбіт |
| Encrypt | 35 | 40 |
| Decrypt | 20 | 26 |

Алгоритми зашифровування «Скелі 512» (функція encrypt)

Параметри:

n – порядок поліному, визначає кількість його коефіцієнтів. Просте число, для якого поліном є незвідним; просте число;

t – натуральне число, яке визначає кількість ненульових елементів малого поліному;

p – менший модуль (p=3) для цього стандарту;

q – більший модуль (просте число);

maxMsgLenBytes – Максимальна довжина повідомлення;

db – довжина випадкового двійкового рядка;

bufferLenBits – довжина буферу для доповненого повідомлення;

octL – довжина кількості октетів для повідомлення визначається параметром octL;

OID – ідентифікатор методу;

minCallsR – кількість викликів функції гешування при формуванні засліплюючого поліному;

minCallsMask – кількість викликів функції гешування при формуванні маскуючого поліному.

Компоненти:

Генератор випадкових чисел (rand);

Функція RE2BSP – перетворення коефіцієнтів полінома в бітовий рядок;

Функція RE2OSP – перетворення коефіцієнтів поліному в рядок октетів;

Функція GenBP – генерація засліплюючого поліному;

Функція MGF – генерація маски.

Вхід:

m – повідомлення для за шифрування (рядок октетів);

mLenBytes – довжина рядка m (кількість октетів);

h – відкритий ключ (більший поліном та відповідний бітовий рядок).

Для обчислення шифртексту необхідно виконати такі або еквівалентні кроки.

1. Перевірка довжини повідомлення.

Якщо mLenBytes > maxMsgLenBytes To

RetValue = ERROR e=0;

2. Формування випадкового рядка b довжиною

3. Формування рядка октетів M довжини *bufferLenBits* .

4. Перетворення рядка октетів M в поліном MTrin за допомогою кодування 3-х бітових рядків в 2 коефіцієнта меншого полінома.

5. Формування рядка октетів sData, який складається з:

OID – ідентифікатор методу;

Повідомлення для за шифрування m;

випадковий рядок b довжиною db бітів (db mod 8 = 0);

байтів відкритого ключа h, перетвореного в рядок байтів за допомогою стандартного компонента для перетворення полінома в рядок бітів RE2BSP, з цього рядка використовуються перші *pkLen бітів*, яка позначена hTrans. Довжина рядка sDataLen=3+*mLenBytes+2*db/8.*

6 Формування засліплюючого полінома r з використанням рядка октетів sData та його довжини r:=BPGM (sData, sDataLen).

7 Обчислення R:=r *h в полі (Z/qZ)[X](X$^n$–X–1).

8 Обчислення R4:=R mod 4.

9 Перетворення R4 в рядок октетів (стандартний компонент RE2OSP). Отримання oR4.

10 Генерація полінома для маскування mask (функція MGF) звикористанням рядка oR4 в якості seed.

11 Обчислення поліному *m'*=(M+mask) mod p.

12 Якщо кількість 1, -1, 0 в поліномі *m'* менше, ніж *tm* то перейти на крок 1.

13 Обчислення шифротексту: *e*:=*R*+*m'* mod *q* (більший поліном).

Перетворення *e* в рядок октетів E (функція RQOS).

Значення, що повертається:

RetValue=OK

шифртекст E (Рядок октетів)

Алгоритми розшифровування «Скеля-512» (функція decrypt)»

Параметри

n – порядок поліному, визначає кількість його коефіцієнтів. Просте число, для якого поліном є незвідним; просте число

t – натуральне число, яке визначає кількість ненульових елементів малого поліному

p –менший модуль (p=3) для цього стандарту

q – більший модуль (просте число)

maxMsgLenBytes – Максимальна довжина повідомлення

db – довжина випадкового двійкового рядка

bufferLenBits – довжина буферу для доповненого повідомлення

octL – довжина кількості октетів для повідомлення визначається параметром octL

OID – ідентифікатор методу

Компоненти:

Функція OS2BSP – перетворення рядка октетів в рядок бітів

Функція RE2BSP – перетворення коефіцієнтів полінома в бітовий рядок

Функція RQOS – перетворення коефіцієнтів полінома в рядок октетів

Функція OSRQ – перетворення рядка октетів E в поліном

Функція GenBP – генерація засліплюю чого поліному

Функція MGF – генерація маски

Вхід:

E –шифртекст (рядок октетів);

mLenBytes – довжина рядка m (кількість октетів)

h – відкритий ключ (більший поліном та відповідний бітовий рядок)

Значення, що повертаються:

1 – Признак успішності (Retvalue=OK, ERROR)

2 – m (розшифроване повідомлення, рядок октетів) в разі успішного завершення

3 – mlen – довжина розшифрованого повідомлення – октетів (разі успішного завершення)

Для обчислення відкритого повідомлення необхідно виконати такі або еквівалентні кроки.

1. Перетворення рядка октетів E в поліном *e* (R/q) – функція OSRQ.

2. Обчислення a:= f * e в полі (Z/qZ)[X](X$^n$–X–1)

3. Обчислення cm' = a mod p

4. Якщо кількість 1, -1, 0 в поліномі *cm'* менше ніж *tm* то

RetValue=Error

m=mlen=0;

Перейти на крок 18.

5. Обчислення cR:=e – m' (mod q) (кандидат на r*h)

6. R4 := cR mod 4

7. Перетворення R4 в рядок октетів (функція RQOS для q=4). Отримання coR4

8. Генерація полінома для маскування mask (функція MGF)

9. Обчислення меншого поліному cmTrin:=cm'–mask (mod p)

10. Перетворення cmTrin в бітовий рядок cM згідно заміни двох коефіцієнтів трьома бітами (табл. 7.1). Якщо для перетворення треба коефіцієнти полінома -1, -1 перетворити в бітовий рядок, то

RetValue = Error

m = mlen = 0;

Перейти на крок 18.

11. Якщо довжина отриманого рядка l mod 8!=0 то видалення з бітового рядка останніх l mod 8 нулів

12. Перетворення бітового рядка Mbin в рядок октетів M (функція BS2OSP)

13. Розібрати рядок октетів M:

13.1 Перші bLen октетів – рядок b

13.2 Наступний байт – довжина повідомлення lm; Якщо lm>maxMsgLenBytes, то

RetValue = Error

m = mlen = 0;

Перейти на крок 18

13.3 Наступні lm байтів – повідомлення m

13.4 Наступні байти – нульові. Якщо ці байти відрізняються від нульових, то

RetValue = Error

m = mlen = 0; Перейти на крок 18

14. Значення, що повертаються: RetValue, m, mlen

Режими роботи

Механізм (алгоритм) асиметричного блокового криптографічного перетворення реалізовано на основі виконання перетворень в кільцях поліномів та скінчених полях. У залежності від довжин (розмірів) загальних параметрів та асиметричних пар ключів (особистого (секретного) та відкритого ключів), застосовуються два режими роботи:

- режим 256 біт захищеності від класичної атаки та 128 біт захищеності від квантової атаки, що позначається як Скеля256/128;
- режим 512 біт захищеності від класичної атаки та 256 біт захищеності від квантової атаки, що позначається як Скеля512/256.

В кожному із режимів роботи за рахунок застосування криптографічних перетворень в кільцях поліномів та скінчених полях забезпечується надання послуг асиметричного шифрування та неспростовності отримувача.

В кожному із вказаних режимів роботи забезпечується захист від атак сторонніми каналами (через витік по технічним каналам).

## Висновки

1. Основною особливістю вимог щодо розроблення проекту національного стандарту АСШ ПІК є забезпечення крім 5-го рівня безпеки, також 7-го рівня – 512 біт класичної криптографічної стійкості та відповідно 256 біт квантової криптографічної стійкості. Причому під 6 рівнем безпеки будемо розуміти забезпечення 384 біт безпеки щодо класичних атак та 192 біт щодо квантових атак. Вказана вимога визначена для всіх складових механізму АСШ ПІК.

2. У криптосистемі «NTRU Prime IIT Ukraine» в якості основного криптоперетворення, як в NTRU Prime, на відміну від NTRU, застосовується перетворення в скінченому полі. Вказане унеможливлює проведення щодо криптографічної системи «NTRU Prime IIT Ukraine» ряду потенційних атак та виключає потенційні слабкості, що присутні криптосистемі NTRU. В основному вони пов'язані з існуванням нетривіальних підкілець чи фактор кілець фактор кільця (зрізаних) поліномів.

3. У криптосистемі «NTRU Prime IIT Ukraine» поліноми $F$ та $r$ є довільними $t$-малими, вони мають 2$t$ ненульових коефіцієнтів (+1, -1) в той час як в NTRU кожен з зазначених поліномів має точно $t$ ненульових коефіцієнтів, які дорівнюють 1 та -1 відповідно. Аналогічне справедливе і для полінома $g$, який використовується у криптосистемі «NTRU Prime IIT Ukraine», – він є довільним малим поліномом з 2$t$ ненульовими коефіцієнтами (+1, -1). Вказане дозволяє розширити у порівнянні з NTRU розмір ключового простору без втрати ефективності реалізації алгоритмів формування ключів та виконання алгоритмів зашифрування і розшифрування.

## Література

[1]. Post-Quantum Cryptography. – Electronic resource. – Access mode: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions.

[2]. Post-Quantum Cryptography. Workshops and Timeline. – Electronic resource. – Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline.

[3]. Yesina Maryna, Olga Akolzina, Olena Kachko (supervisor). Proposals of the expert estimations technique usage for the comparing and estimation NTRU-like cryptographic systems // Inżynier XXI wieku ("Engineer of XXI Century" – the VII Inter University Conference of Students, PhD Students and Young Scientists: University of Bielsko-Biala, Poland, December 08, 2017). – Bielsko-Biała: Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Białej, 2017. – P. 383–398. – ISBN 978-83-65182-81-4 (Tom 2) – Chapter in monograph. (Розділ в монографії).

[4]. Gorbenko I. D. General statements and analysis of the end-to-end encryption algorithm NRTU Prime IIT Ukraine / I. D. Gorbenko, O. G. Kachko, M. V. Yesina // Радиотехника. – Х. : Харьковский национальный университет радиоэлектроники, 2018. – Выпуск 193 – С. 5–16.