УДК 004.056.55
DOI: 10.32626/2308-5916.2019-19.120-125

В. В. Онопрієнко*, канд. техн. наук, доцент,
В. А. Пономар,** канд. техн. наук

* ПАТ «Інститут інформаційних технологій», м Харків,
**Харківський національний університет імені В. Н. Каразіна, м. Харків

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОСТКВАНТОВИХ АСИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Робота присвячена аналізу кандидатів на постквантовий стандарт асиметричного шифрування. З розвитком технологій квантових обчислень і появою квантового комп'ютера виникає загроза поточному стану захищеності криптографічних систем з відкритим ключем. З появою квантового комп'ютера, який буде мати необхідний для методів квантового криптоаналізу об'єм регістру розподілених квантів, стійкість існуючих криптоалгоритмів значно знизиться. З цього випливає необхідність створення алгоритмів стійких до методів квантового криптоаналізу. Європейський проект «Нові європейські алгоритми для електронного підпису, цілісності та шифрування» (NESSIE) та Національний інститут стандартів і технологій (NIST) США об'явили про початок набору претендентів на конкурс постквантових алгоритмів, стандарти щодо яких планується прийняти в 2020–2022 рр. Для порівняння обрано методику оцінювання на основі інтегральних оцінок безумовних і умовних критеріїв. Аналіз проводився серед алгоритмів, що пройшли загальні безумовні критерії. Як умовні критерії обрано чисельні характеристики алгоритмів. Крім того висувалися додаткові безумовні критерії.

Актуальна задача — це порівняльний аналіз та оцінка можливості використання постквантових механізмів, які представлені існуючими на даний момент алгоритмами, в залежності від умов застосування. На даний момент проводиться лише дослідження можливості використання відповідних криптоперетворень у постквантовий період, але що не проводився аналіз переваг одних над іншими. Крім того необхідно оцінити саму можливість використання таких алгоритмів з урахуванням обмежень, що накладаються існуючими інформаційними системами.

Результати досліджень дозволяють зрозуміти поточний стан розвитку постквантових криптоалгоритмів і спрогнозувати можливий їх подальший розвиток. Цей прогноз важливий тим, що постквантові криптографічні механізми являють собою новий етап розвитку та застосування криптографії. Крім того практичне значення дослідження полягає в отриманні оцінки постквантових алгоритмів.

Ключові слова: *постквантові криптографічні алгоритми, порівняльна оцінка криптоалгоритмів, критерії порівняння криптоалгоритмів.*

Вступ. Останнім часом все більшої актуальності набуває питання захисту інформації від атак з використанням квантового комп'ютера. Це питання постає через те, що за останніми дослідженнями, захист класичних криптографічних алгоритмів електронного підпису від методів квантового криптоаналізу буде значно меншим. Тому постає необхідність створення нових алгоритмів підпису та шифрування, що буде використовувати криптографічні перетворення, що є стійкими до методів квантового криптоаналізу. Але додатково висувається вимога до механізмів захисту ключів за допомогою алгоритмів інкапсуляції ключів.

Як підтвердження необхідності розробки постквантових алгоритмів необхідно привести роботу [1]. В ній відмічається, що в серпні 2015 року агентство національної безпеки (АНБ) уряду США виступило з великою заявою про необхідність розробки стандартів пост квантової криптографії. В цій статті проаналізована небезпека застосування квантових комп'ютерів для сучасних криптоалгоритмів, та запропоновано механізми криптоперетворень, що є стійкими до квантового криптоаналізу різних типів.

Аналіз літературних джерел [1–3] показав, що нині ще відсутні порівняння між потенційно можливими постквантовими механізмами, а також дані про можливості їх застосування в залежності від умов та середовища. Водночас саме вибір найбільш перспективних криптографічних перетворень для пост квантового застосування є надзвичайно важливим, так як він визначить подальший напрямок розвитку криптографії асиметричної криптографії.

Метою досліджень є оцінка та порівняльний аналіз існуючих методів постквантових криптоперетворень алгоритмів у залежності від висунутих вимог та умов їх застосування. Це надасть можливість, по-перше, виділити алгоритми, які скоріше за все стануть майбутніми постквантовими стандартами, а по-друге — спрогнозувати подальший напрямок розвитку асиметричної криптографії.

Матеріали та методи дослідження. При порівняльному аналізі використовувалася сукупність безумовних і умовних оцінок. Умовними оцінками виступали наступні характеристики алгоритмів:

1) $I_{ст.}$ — рівень криптографічної стійкості;
2) $l_{в.к}$ — довжина відкритого ключа;
3) $l_{о.к}$ — довжина особистого ключа;
4) $l_{рез.}$ — довжина результату криптоперетворення;
5) $T_{пр.}$ — швидкість прямого криптоперетворення;
6) $T_{зв.}$ — швидкість зворотнього криптоперетворення;
7) $T_{гкп.}$ — швидкість генерації ключової пари.

При оцінюванні використовувався метод попарних порівнянь. Експертні оцінки використовувалися для оцінки важливості кожної з наведених характеристик, а безпосередньо при порівнянні алгоритмів

використовувалися об'єктивні числові значення, шкала оцінки (яка при оцінювані об'єктивних показників характеристик враховує порядок переваги одного алгоритма над іншим за цією характеристикою), та вагові коефіцієнти важливості характеристик, що були отримані при експертному оцінюванні (табл. 1).

Таблиця 1

Експертні оцінки характеристик криптоалгоритмів

Показники / Експерти	$I_{ст.}$	$l_{в.к}$	$l_{о.к}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гкп.}$
1	0,073	0,045	0,033	0,262	0,275	0,275	0,038
2	0,067	0,067	0,029	0,198	0,298	0,298	0,043
3	0,080	0,035	0,035	0,341	0,229	0,229	0,053
4	0,098	0,051	0,029	0,390	0,205	0,205	0,023
5	0,083	0,083	0,039	0,386	0,191	0,191	0,027
W	0,080	0,056	0,033	0,315	0,239	0,239	0,037

В даному дослідженні при виборі алгоритмів висувалися додаткові безумовні вимоги:

1) алгоритм має гарантувати, що найменше 3 рівень безпеки за класифікацією NIST [3];
2) якщо існує декілька варіантів наборів параметрів для одного алгоритму, то в порівнянні бере участь варіант, що гарантує найбільшу безпеку.

В табл. 2 наведені характеристики обраних для порівняння алгоритмів, швидкодія задана в мільйонах (10^6) тактів.

На рис. 1 показано гіксограму відносної переваги алгоритмів. Як видно найбільшу перевагу має алгоритм NTRU Prime IIT Ukraine, на другому місці — LAC, на третьому — OKCN/AKCN/CNKE.

Для уточнення результатів проведено порівняння з використанням методу ранжування. Відмінність цього методу в тому, що він враховує лише кількість характеристик за якими у алгоритма є перевага та кількість алгоритмів над якими за цією характеристикою він кращий, але не враховує розмір цієї переваги.

Таблиця 2

Характеристики алгоритмів шифрування

Алгоритми	Тип	$I_{ст.}$	$l_{в.к}$	$l_{о.к}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гкп.}$
Giophantus	Lattices	5	27204	1134	54408	420,543	792,577	0,213
KINDI	Lattices	5	2368	2752	3328	0,705	0,919	0,489
LAC	Lattices	5	1056	2080	2048	0,137	0,133	0,573
LEDApkc	Codes	5	12384	40	24768	92,84	264,938	0,810
LIMA	Lattices	5	12289	18433	12291	0,909	1,126	1,084
Lizard	Lattices	5	8192	998266	8512	0,805	0,568	1,307
LOTUS	Lattices	5	1470976	1630720	1768	0,901	1,087	3,057

Продовження таблиці 2

McNie	Codes	5	630	584	729	3,504	7,707	4,239
NTRUEncrypt	Lattices	5	64232	63912	127696	174,2	0,299	47,297
Odd Manhattan	Lattices	5	4454241	4456650	616704	141,625	155,302	127,488
OKCN/ AKCN/ CNKE	Lattices	5	1312	992	1200	0,568	0,631	366,432
Round2	Lattices	5	830	1039	953	0,905	1,135	1599,640
RQC	Codes	5	40	1795	3574	6,46	18	1899,306
Titanium	Lattices	5	23552	32	8320	2,974	0,561	2147,483
NTRU Prime IIT Ukraine	Lattices	5	1578	243	1578	0,074	0,138	3248,122

В табл. 3 наведені експертні оцінки та вагові коефіцієнти важливості характеристик криптографічних алгоритмів асиметричного шифрування.

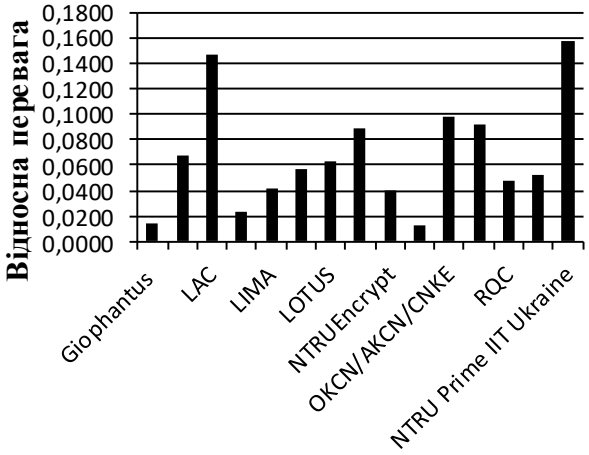

Рис. 1. *Відносна перевага алгоритмів асиметричного шифрування*

Таблиця 3

Експертні оцінки характеристик криптоалгоритмів за методом ранжування

Показники / Експерти	$I_{ст.}$	$l_{в.к}$	$l_{о.к}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гкп.}$
1	4	3	1	5	6	7	2
2	3	4	1	5	6	7	2
3	4	2	1	7	5	6	3

Продовження таблиці 3

4	4	3	2	7	6	5	1
5	4	3	2	7	6	5	1
W	0,136	0,107	0,050	0,221	0,207	0,214	0,064

На рис. 2 показано гіксограму відносної переваги алгоритмів, що отримано методом ранжування. Як видно найбільшу перевагу мають алгоритми NTRU Prime IIT Ukraine та LAC (в них однакове значення переваги), на третьому — OKCN/AKCN/CNKE.

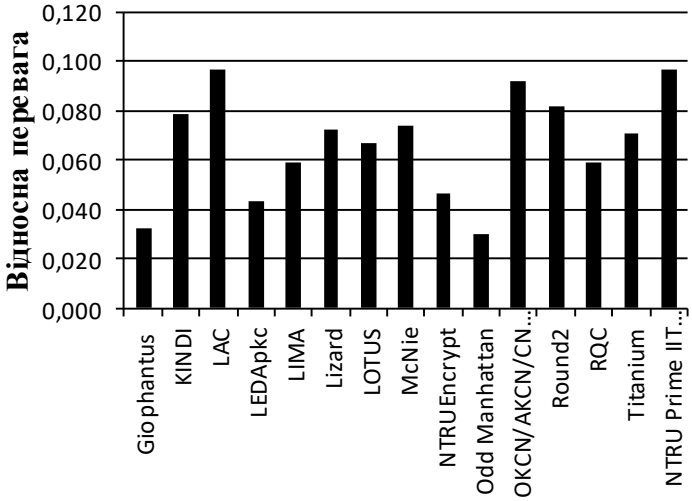

Рис. 2. *Відносна перевага алгоритмів асиметричного шифрування за методом ранжування*

Висновки. З результатів порівняння постквантових алгоритмів шифрування максимального рівня захисту можна зробити висновок, що алгоритми, що базуються на криптоперетвореннях у решітках числового поля мають перевагу над алгоритмами з іншими математичними апаратами, що дозволяє зосередити увагу над дослідженням саме цих алгоритмів.

Список використаних джерел:

1. Koblitz N., Menezes A. J. A riddle wrapped in an enigma. URL: https://eprint.iacr.org/2015/1018.pdf.
2. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. *The Seventh International Conference on Post-Quntum Cryptography*, Japan, 2016. URL: https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf.
3. Mosca M. Setting the Scene for the ETSI Quantum-safe Cryptography Workshop. *E-proceedings of «1st Quantum-Safe-Crypto Workshop»*, Sophia Antipolis, Sep 26–27, 2013. URL: http://docbox.etsi.org/Workshop/2013/-201309_CRYPTO/eproceedings_Crypto_2013.pdf.

COMPARATIVE ANALYSIS OF POST-QUANTUM ASYMMETRIC ENCRYPT ALGORITHMS

Due to the development of technologies for quantum computing and the introduction of quantum computer, there is a threat to the current state of protection of cryptographic systems with a public key. With an advent of quantum computer that would have the volume of register required for the methods of quantum cryptanalysis, the stability of existing crypto algorithms will significantly degrade. This necessitates the creation of algorithms resistant to the methods of quantum cryptanalysis. The European project «New European Schemes for Signatures, Integrity, and Encryptions» (NESSIE) and the National Institute of Standards and Technologies (NIST) of the USA announced a start of recruiting the applicants for the contest of post-quantum algorithms whose standards are planned to be adopted over 2020–2022. In order to compare, a procedure for evaluation was selected based on integral assessments of unconditional and conditional criteria. An analysis was conducted among the algorithms that fulfilled general unconditional criteria. As conditional criteria, we chose numerical characteristics of algorithms. In addition, additional unconditional criteria were put forward.

A relevant task is the comparative analysis and evaluation of a possibility to use the post-quantum mechanisms, which are represented by the algorithms that already exist, depending on the conditions of applying them. At present, only the possibility of using the appropriate crypto transformations over a post-quantum period is being examined, but the analysis of advantages of one over another has not been run yet. In addition, it is necessary to evaluate the very possibility to use such algorithms taking into account those constraints that are imposed by the existing information systems.

Results of present research allow us to understand current state in the development of post-quantum crypto algorithms and to predict their possible further development.

This forecast is important in that the post-quantum cryptographic mechanisms represent a new stage in the development and use of cryptography. In addition, the practical value of the research consists in obtaining the evaluation for post-quantum algorithms.

Key words: *post-quantum cryptographic algorithms, comparative assessment of crypto algorithms, comparison criteria of crypto algorithms.*

Одержано 12.02.2019