11. Zeng K., Yang C., Wei D., and Rao T.R.N. «Pseudo-random bit generators in stream-cipher cryptography». Computer. 1991.
12. David R. Random Testing of Digital Circuits. New York: Marcel Dekker. 1998.
13. Massey J. L. «Shift-register synthesis and BCH decoding». IEEE Transactions on Information Theory, Vol. 15. 1969. P. 122–127.
14. Dubrova E., Teslenko M., and Tenhunen H. «On analysis and synthesis of (n,k)-non-linear feedback shift registers», in Design and Test in Europe. 2008. P. 133–137.
15. Коробейников А. Г., Гатчин Ю. А. Математические основы криптологии. Учебное пособие. Санкт-Петербург. 2004. Режим доступа: http://books.ifmo.ru/file/pdf/56.pdf.
16. Полуяненко Н. А., Потий А. В. Сравнение объема ансамбля М-РСЛОС и М-РСНОС, скорости генерации на их основе, для GF(2) и в расширениях поля GF(22). *Радиотехника.* Всеукраинский межведомственный научно-технический сборник. 2016. № 186/216. С. 153–160.

In this paper, one of the important elements of generator of stream ciphers — the nonlinear feedback shift registers (NLFSR) are considered. NLFSR with nonlinearity of random order are considered. The amount of different forming polynomials that can be used for NLFSR are studied. The result — calculated equations for determination of the number of NLFSR of random and maximal order (for a given size of the register) are showed.

Key words: *stream ciphers, nonlinear systems, SRNLF.*

Получено 24.03.2017

УДК 004.056.055

В. А. Пономар, аспірант

Харківський національний університет імені В. Н. Каразіна, м. Харків

СТАН, МЕТОДИКА ТА ПРОМІЖНІ ПІДСУМКИ РОЗРОБКИ ПРОЕКТІВ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Наводяться вимоги, пропозиції з порівняння та проміжні результати порівняння кандидатів у постквантові стандарти асиметричних крипто перетворень.

Ключові слова: *асиметричні крипто перетворення, методи порівняння, проміжні результати порівняння постквантових крипто примітивів в ході конкурсу NIST США.*

Вступ. В 2015–2016 роках відбувся ряд значущих подій, які уже суттєво вплинули на інтенсивний розвиток постквантової криптографії. NIST США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів електронного підпису та асиметричного направленого шифрування, які будуть актуальними та можуть застосовуватись

у постквантовий період, оголосив конкурс на розробку стандартів постквантових асиметричних криптографічних примітивів [1, 3, 4].

Мета роботи — це аналіз стану, основних вимог, обгрунтування системи критеріїв та методичних основ порівняння та викладення проміжного стану порівняльного аналізу постквантових стандартів асиметричних криптографічних перетворень.

1. Стан розроблення та застосування методик порівняльного аналізу криптографічних примітивів. Одна із найбільш важливих проблем у процесі проведення конкурсу — це застосування об'єктивних методів, методика оцінювання, порівняльний аналіз криптографічних примітивів. В поданні [2] методи та методика порівняльного аналізу симетричних та асиметричних крипто примітивів. Вони базуються на використанні системи безумовних та умовних часткових та інтегральних критеріїв. Основним завданням таких методик є формалізація процесів прийняття рішень та зменшення впливу суб'єктивних факторів.

2. Критерії та показники оцінки крипто примітивів. Наші попередні дослідження дозволили зробити висновок, що порівняння криптографічних примітивів можна здійснити з використанням двох сукупностей критеріїв: безумовних та умовних. Такий підхід, дозволяє зробити оцінку та порівняння крипто перетворень, що є кандидатами у 2 етапи. Такий підхід ґрунтується, в тому числі, і на врахуванні чи використанні експертних оцінок [2].

На першому етапі спочатку перевіряється відповідність крипто перетворення системі часткових безумовних критеріїв, а потім обчислюється безумовний інтегральний критерій.

На другому етапі отримуються відповідні оцінки з використанням часткових умовних критеріїв, а потім на їх основі обчислюється інтегральний умовний критерій.

3. Безумовні та умовні критерії оцінки постквантових криптографічних примітивів. До безумовних критеріїв будемо відносити ті критерії, виконання яких для криптографічного примітиву є обов'язковим, тобто безумовними [4, 5].

В табл. 1 наведено систему безумовних критеріїв, що пропонуються для використання в процесі конкурсу [2].

Таблиця 1

Безумовні критерії оцінки ЕП та НШ

Безумовні критерії	**Позначення**
Надійність, простота та прозорість математичної бази постквантових крипто перетворень ЕП та НШ	W_1
Практична захищеність крипто для моделі безпеки IND–CCF2	W_2
Практична захищеність крипто перетворення типу ЕП від відомих атак для моделі EUF–CMA	W_3

Продовження таблиці 1

Обгрунтованість реальної стійкості крипто перетворень на основі загальних параметрів та ключів	W_4
Теоретична захищеність крипто перетворень для моделей EUF–CMA (ЕП) та IND–CCF2 (НШ)	W_5
Можливість заміни стандартизованих крипто примітивів на постквантові та їх застосування	W_6
Допустима складність прямого $I_{пр}$ та зворотного $I_{зв}$ крипто перетворень та генерування пар ключів $I_{кл}$	W_7
Виконання обмежень на мінімальну та максимальну довжини та відсутність слабких ключів	W_8

З урахуванням наведених у таблиці часткових безумовних критеріїв $W_1 - W_8$ та умови функцію відповідності крипто перетворення вимогам інтегрального безумовного критерію:

$$fi() = W_1 \wedge W_2\,(W_3) \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7 \wedge W_8 = W_\delta\,(1),$$

де символ « $\wedge$ » позначає операцію кон'юнкції булевих змінних.

4. Умовні критерії оцінки криптографічних перетворень типу ЕП та НШ. Якісне й кількісне порівняння крипто перетворень можна здійснити, використовуючи часткові умовні та узагальнені критерії [2]. В табл. 2 наведено перелік критеріїв, вимоги і NIST [3].

Таблиця 2

Умовні критерії оцінки ЕП та НШ

Умовні критерії	**Позначення**
Додаткові властивості безпеки: «perfect forward secrecy» (удосконалена пряма безпека); стійкість до атак сторонніми каналами; до мультиключових атак, відмов	*K*1
Вимоги до стійкості 1) 128(192, 256) біт класичної безпеки / 64(128,192) біт квантової; 2) 128 (192,256) біт класичної безпеки / 80(256, 384,512) біт квантової захищеності (SHA-256/ SHA3-256)	*K*2
Додаткові вимоги до стійкості 3) 512 біт класичної безпеки / 256 біт квантової захищеності (SHA2/ SHA3-512, ДСТУ 7564: 2014 — 512 біт) 4) 512 біт класичної безпеки /від 128 до 256 біт квантової захищеності (ДСТУ 7624:2014 (Калина — 512))	*K*3
Помилки шифрування, низький відсоток помилок	*K*4
Можливість багаторазового НШ чи ЕП	*K*5
Гнучкість: додатково оптимізація, неявний обмін ключами, кросплатформеність; розпаралелювання	*K*6
Перевірка на коректність опорних та оптимізованих реалізацій	*K*7
Ефективність: обчислення часу генерації ключа, зашифрування, розшифрування, цифрового підпису	*K*8
Випробувань. Основні платформи: NIST PQC Reference Platform; Intel x64; Windows or Linux; 8-бітових та сигнальних процесорів, виділених CMOS, тощо	*K*9

Продовження таблиці 2

Можливість і умови вільного поширення постквантових крипто перетворень ЕП чи НШ	$K10$
Рівень довіри до постквантових ЕП чи НШ	$K11$
Перспективність та виправданість ЕП чи НШ	$K12$

5. Моделі порушника та загроз. Аналіз показав, що квантовий комп'ютер можна розглядати як основну модель порушника, а методи та алгоритми, що реалізуються на квантовому комп'ютерові, моделлю загроз.

На наш погляд друга проблемна задача успішно вирішується. Так на сьогодні вже існують квантові методи та розроблені на їх основі алгоритми, які дають змогу проводити атаки на асиметричні криптосистеми RSA, DSA, ECC та NTRU [2, 5, 6]. До них, в першу чергу, необхідно віднести [2, 5, 6] такі квантові алгоритми як: квантовий алгоритм Гровера; алгоритм факторизації Шора; алгоритм Шора дискретного логарифму; алгоритми Ванга тощо.

Враховуючи поспішність, з якою США та ЄС, приступили до побудови постквантових комп'ютерів і досягнення, він з'явиться в явному вигляді безпосередньо. Так в «1000-кубітном» комп'ютері кубіти в дійсності організовані в кластери по 8 кубіт кожен.

6. Попередній аналіз асиметричних постквантових крипто перетворень. У табл. 3 наведені загальні характеристики математичного апарату, на яких грунтуються механізми ЕП, з використанням яких можуть бути розроблені квантово-захищені алгоритми ЕП [1–4, 8].

Таблиця 3

Напрямки квантово-захищені асиметричні алгоритми [1–6]

Криптографічна схема	**Підпис**	**Шифрування**	**Розмір ключа**	**Тип даних**	**Core Ops.**	**Cryptographic Maturity**
Hash-Based	Yes	No	≈20	Hash out.	Hashing	High
Multivariate Quadratic	Yes	No	≈10k	$GF(2^m)$	Matrix LSE	Low, medium schemes
L-B: NTRU General lattice	Maybe Maybe	Yes Yes	<0.1k ≈100k	Z_q $GF(2^m)$	Matrix mult. Matrix mult.	Medium Medium
Code-Based	Expensive	Yes	≈100k	$GF(2^m)$	Matrix mult.	High, with prec. to impl.

Наведені в табл. 4 механізми ЕП запропоновані ETSI для подальшого вивчення і дослідження у якості можливих кандидатів на квантово-захищені схеми ЕП.

Таблиця 4

Порівняння довжин ключів та підписів для квантово-захищених алгоритмів ЕП

Тип	Схема	Безпечність (біти)	Відктирий ключ (байти)	Підпис (байти)
Lattice	Lyubashevsky	-------	1 664	2 560
	NTRU-MLS	128	988	988
	Aguilar et al	128	1 082	1 894
	Guneysu te al	80	1 472	1 120
	BLISS	128	896	640
MQ	Quartz	80	72 237	16
	UOV	128	413 145	135
	Cyclic-UOV	128	60 840	135
	Rainbow	128	139 363	79
	Cyclic-Rainbow	128	48 411	79
Code	Parallel-CFS	120	503 316 480	108
	Cayrel et al	128	10 920	47 248
	RankSign	130	7 200	1 080
	Cyclic- RankSign	130	3 538	1 080
Hash	Merkle	128	32	1 731
	Leighton-Micali	128	20	668
	XMSS	256	64	8 392
	SPHINCS	256	1 056	41 000
Isogeny	Jao-Soukharev	128	768	1 280
	Sun-Tian-Wang	128	768	16

Аналіз даних, що наведені в табл. 3 та 4, дозволяє зробити висновок про переваги та недоліки окремих крипто перетворень.

7. Обґрунтування параметрів та ключів при порівнянні. В процесі досліджень отримані попередні результати порівняння доступних постквантових алгоритмів. Обмеження використані у зв'язку з відсутністю повної інформації (табл. 5).

Таблиця 5

Показники та властивості постквантових крипто примітивів

Параметри / алгоритми	1) крипторафічна стійкість	2) довжина відкритого ключа	3) довжина особистого ключа	4) довжина підпису	5) швидкість прямого перетворення	6) швидкість зворотнього перетворення
1. NTRU	128	988	256	988-	0,5	0,02
2. BLISS	128	896	256	640	0,02	0,02
3. Quartz	80	72237	3000	16	2	0,05
4. XMSS	128	1700	280	2083	2	0,2
5. SPHINCS	128	1056	1088	41000	2	0,2
6. RankSign	130	7200	21600	1080	0,02	0,02
7. Jao-Souk	128	768	768	1280*	5	5

Використано порівняння за безумовними критеріями для різних сфер застосування. Як критерії використані: а) $l_{в.к}$ — довжина відкритого ключа; б) $l_{о.к}$ — довжина особистого ключа; в) $l_{рез.}$ — довжина результату крипто перетворення; г) інтерактивність.

Ці критерії відрізняються особливістю наступних випадків.

8. Порівняльна оцінка застосування криптографічних алгоритмів. В табл. 6 наведено результат визначення вагових коефіцієнтів за експортними оцінками для механізмів електронного підпису для криптографії стандартних АС (табл. 5).

Таблиця 6

Вагові коефіцієнтів механізмів стандартного підпису

Критерії	**1**	**2**	**3**	**4**	**5**	**6**
1	0,266	0,177	0,124	0,080	0,177	0,177
2	0,204	0,275	0,068	0,110	0,140	0,204
3	0,138	0,232	0,054	0,083	0,138	0,354
4	0,134	0,229	0,062	0,134	0,089	0,352
5	0,153	0,089	0,058	0,274	0,153	0,274
W	0,179	0,200	0,073	0,136	0,139	0,272

Рівень узгодженості оцінок 0,3, що задовольняє вимогам. Після проведення оцінок алгоритм BLISS має рівень 0,763, XMSS — 0,237.

В табл. 7 наведено результат визначення вагових коефіцієнтів механізмів шифрування в хмарному середовищі.

Таблиця 7

Вагові коефіцієнти шифрування для криптографії в хмарі

Критерії	**1**	**2**	**3**	**4**	**5**	**6**
1	0,319	0,068	0,068	0,182	0,182	0,182
2	0,233	0,055	0,082	0,164	0,233	0,233
3	0,329	0,064	0,107	0,107	0,196	0,196
4	0,243	0,058	0,085	0,136	0,234	0,243
5	0,246	0,062	0,062	0,140	0,246	0,246
W	0,274	0,061	0,081	0,146	0,218	0,220

Рівень узгодженості оцінок 0,3, що задовольняє вимогам. Після проведення оцінок алгоритм NTRU має рівень 0,684, Jao-Sukharev — 0,316.

Висновки.

1. При порівнянні постквантових алгоритмів пропонується використовувати системи безумовних та умовних часткових та інтегральних критеріїв.
2. Квантовий комп'ютер можна розглядати як основну модель порушника, а методи та алгоритми моделлю загроз.

3. У табл. 3 наведені загальні характеристики математичного апарату, на яких грунтуються механізми ЕП
4. У табл. 6, 7 наведені попередні результати, що отримані з використанням запропонованої методики.

Список використаних джерел:

1. Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. Режим доступу: http://www.nist.gov/pqcrypto.
2. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем: Монографія: за заг. ред. професора І. Д. Горбенко. Харків: Форт, 2015. 959 с.
3. Moody D. Post-Quntum Cryptography: NIST's Plan for the Future. Japan, 2016. Режим доступу: https://pqcrypto2016.jp/data/ pqc2016_nist_announcement.pdf
4. ETSI GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework.
5. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Text]. SIAM J. Comput. 1997. 26 (5). P. 1484–1509.
6. Grover L. K. A fast quantum mechanics algorithm for database search [Text]. Proceeding of the.
7. Wang H., MA Zhi, MA ChuanGui. An efficient quantum meet-in-the-middle attack against NTRU-2005 [Text]. Chinese Science Bulletin. 2013. Vol. 58, N 28–29. P. 3514–3518.
8. Горбенко І. Д., Кузнєцов О. О., Потій О. В., Горбенко Ю. І., Ганзя Р. С., Пономар В. А. Постквантова криптографія та механізми її реалізації. *Радиотехника*. 2016. Вып. 186. С. 32–52.

This article deals with requirements, proposals, comparison and intermediate comparison results of candidates for the post quantum crypto standards of asymmetric transformations.

Key words: *asymmetric crypto transformation, methods of comparison, intermediate comparison results of post quantum crypto primitives in the competition NIST USA.*

Одержано 20.02.2017