УДК 004.056.55

О. Г. Качко*, канд. техн. наук, професор,
Л. В. Макутоніна,** канд. техн. наук, с. н. с.,
О. С. Акользіна,** магістр

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

ОПТИМІЗАЦІЯ NTRU ПОДІБНОГО АЛГОРИТМУ ДЛЯ НЕСИМЕТРИЧНОГО ШИФРУВАННЯ З «НЕЗРУЧНИМИ ПАРАМЕТРАМИ»

Досліджено новий клас параметрів NTRU подібного алгоритму, оптимізовані основні алгоритмічні операції.

Ключові слова: *NTRU подібні алгоритми, обчислювальна складність, часова продуктивність.*

Вступ. В зв'язку зі значними успіхами, досягнутими при розробці квантових комп'ютерів суттєво виріс інтерес до алгоритмів, криптографічна стійкість яких базується на криптографічній стійкості алгебраїчних решіток. Саме до цього класу відносяться NTRU подібні алгоритми.

Однією з головних характеристик стандарту NTRU [1] є мала потреба в ресурсах, і, перш за все, порівняно невелика обчислювальна складність. Це досягається за рахунок обрання параметрів: поліном $X^N - 1$ та $q = 2048$, для яких обчислення модулю фактично не потрібно. Деякі атаки на алгоритм використовують спеціальний вид параметрів, прийнятих в [1].

В роботі [2] запропоновано клас параметрів, для яких не відомі атаки, пов'язані з їх структурою. Цей клас параметрів включає незвідний поліном $x^p - x - 1$ та просте число $q > p$.

1. Опис основних алгоритмів стандартизованого NTRU-методу. Під час дослідження нового класу системних параметрів використовувався класичний стандартизований NTRU метод. Для більш легкого розуміння одержаних результатів дамо короткий опис алгоритмів зашифрування і розшифрування відносно [1, с. 37–42].

1.1. Алгоритм зашифрування. Задаються параметри: N, q, *db* (довжина випадкової послідовності в бітах) та *pkLen* (довжина частини відкритого ключа), *OID* — ідентифікатор (3 байти), *dm0*- мінімальна кількість 1 і -1 для поліному, який відповідає повідомленню для шифрування, *MinCallMask*, *MinCallR* — мінімальна кількість викликів функції хешування для формування поліному для маскування та сліпого поліному відповідно, та *maxMsgLenBytes* — максимальна довжина повідомлення. Вхідними даними є: повідомлення для шифру-

вання m довжиною l байтів, відкритий ключ одержувача h. На виході маємо зашифроване повідомлення, представлене у вигляді масиву байтів e, його довжину, або помилку зашифрування.

Для зашифрування виконуються наступні кроки:

1. Перевірка довжини повідомлення для шифрування. Якщо $l > maxMsgLenBytes$, то повертається помилка.
2. Генерація випадкової послідовності b довжиною db бітів.
3. Формування рядка: $M = b \,||\, l \,||\, m$ та його доповнення $maxMsgLenBytes + 1$ нулями.
4. Формування $Mbin$ поліному за рахунок перетворення 3-х бітів вхідної послідовності в 2 коефіцієнта поліному.
5. Формування рядка $sData = OID \,||\, m \,||\, b \,||\, hTrunc$, де $hTrunc$ — початкові біти відкритого ключа довжиною $pkLen$.
6. Формування сліпого поліному r за допомогою IGF алгоритму IGF ($sData$, N, c, $minCallsR$).
7. Обчислення $R = r * h \bmod q$.
8. Обчислення $R4 = R \bmod 4$ та формування відповідного рядка байтів $oR4$.
9. Генерація поліному для маскування $mask = MGF$ ($oR4$, $minCalMask$).mod 3.
10. Обчислення $m' = M + mask$ та визначення кількості 1 (–1) в m'. Якщо кількість 1 або $-1 < dm0$, то повернутися на крок 2.
11. Обчислення $e' = R + m' \pmod q$.
12. Перетворення поліному e' в рядок байтів e.
13. Результат: рядок e та його довжина.

1.2. Алгоритм розшифрування. Задаються параметри: N, q, p, db, OID, $pkLen$, $dm0$, $maxMsgLenBytes$, $minCallMask$, нижня межа коефіцієнту зашифрування A. Вхідними даними є: особистий ключ одержувача f, відкритий ключ відправника h, зашифроване повідомлення представлене масивом байтів e, та його довжина l. На виході маємо розшифроване повідомлення m, або помилку розшифрування.

Для розшифрування виконуються наступні кроки.

1. Перетворення рядка байтів e в поліном e'.
2. Обчислення поліному $a := f * e'$ зі $(Z/qZ)[X]/(X^N - 1)$ зі коефіцієнтами, які зводяться в інтервалі $[A, A + q - 1]$.
3. Обчислюється $m' = a \bmod 3$.
4. Якщо кількість 1 (–1) в m' менше ніж $dm0$, то повертається помилка.
5. Обчислюється $R' = e - m'$.
6. Обчислюється $R4' = R \bmod 4$.
7. Перетворення поліному $R4'$ в рядок байтів $oR4'$.

8. Обчислення поліному для маскування *mask'*= *MGF*(*oR*4, *N*, *minCallMask*).
9. Обчислюється *Mtrinє* = (*m'* – *mask'*) mod 3.
10. Перетворення поліному в рядок байтів, 2 коефіцієнта полінома перетворюються в 3 біта. Якщо сусідні коефіцієнти поліному в парі дорівнюють –1, то повертається помилка. Отримаємо рядок *M*.
11. Перші *db* байтів — випадкова послідовність *b*, далі довжина повідомлення після розшифрування *l'* = *M*[*db*]. Якщо *l'* > *maxMsgLenBytes*, то повертається помилка.
12. Виділення повідомлення *m*, що розшифроване. Воно розташовано після довжини та займає *l'* байтів.
13. Перевірка решти байтів, вони повинні бути нульовими. Якщо це не так, то повертається помилка.
14. Формування *sData'*= *OID* || *m* || *b* || *hTrunc* , де *hTrunc* — початкові біти відкритого ключа довжиною *pkLen.*
15. Формування сліпого поліному *r* за допомогою IGF алгоритму IGF (*sData'*, *N*, *c*, *minCallsR*).
16. Обчислення *R''* = *r* * *h* mod *q*.
17. Якщо *R'*! = *R''*, тоді повертається помилка.
18. Повертається *m* та його довжина *l.*

2. Аналіз результатів досліджень. Нами було проаналізовано NTRU метод із змінними параметрами [2], який є перспективною модифікацією класичного NTRU методу. Пропонований набір параметрів у роботі [2] має покращені показники захищеності і відповідає сучасним вимогам NIST до пост квантових алгоритмів [3], але за рахунок збільшення операцій гешування, зміненої процедури множення поліномів, а також у зв'язку з зміненими поліномами та взагалі зі зміною усіх параметрів системи, показники швидкодії є дещо слабкішими під час виконання процедури зашифрування.

Стандартизований метод використовує параметри у кільці зрізаних поліномів $(Z/q)[x]/(x^p-1)$, а метод зі модифікованими параметрами $(Z/q)[x]/(x^p-x-1)$.

Результати досліджень відносно оптимізації процедури множення поліномів, а також оптимізації обчислення сліпого поліному *r* для NTRU методу зі модифікованими, незручними параметрами зведені у табл. 1; нами виконувалися дослідження для усіх 123 наборів параметрів, але для полегшення сприймання одержаних результатів у табл. 1 і табл. 2 були занесені деякі дані для рівнів безпеки 192 і 256, значення наведені над подвійною рискою відносяться до рівня безпеки 192, а під нею — до рівня безпеки 256.

Таблиця 1

Швидкісні показники основних операцій методу з модифікованими параметрами

p	*q*	**Показники швидкодії операцій шифрування у тактах процесора**				
		Зашифрування			**Розшифрування**	
		b	**Mul**	**ToBytes**	**ToPol**	**Mul**
673	9413	67659	97225	61059	1942	99929
691	6449	54684	70511	61577	2105	73846
719	9133	76744	101816	64673	2096	130892
727	5827	48665	68339	65611	2142	97825
739	9829	81011	111582	67402	2084	112317
743	7541	59895	88110	67429	2187	88600
757	7879	62780	94146	68490	2312	100672
761	7883	63938	97523	128709	2232	95147
769	6599	53081	81011	69897	2296	82645
773	9811	80249	118925	70469	2256	162804
787	4243	36801	56250	71182	2314	56798
809	6113	49900	79411	102198	2436	84508
811	8543	64166	106165	73454	2269	164512
823	8069	61278	105412	75525	2415	140741
827	9767	76814	122446	74500	2311	122724
853	9721	70356	124874	77028	2304	125549
857	5167	45015	106236	104195	2498	100377
863	8779	63681	114128	76547	2492	142881
881	3217	61551	52540	84976	2104	76580
941	2521	26842	42266	85914	2108	40872
947	3917	35204	60936	86238	2138	57977
1009	4259	36638	69594	89961	2970	68998
1013	3923	35930	64547	91863	2168	65215
883	8089	59087	108340	79913	2437	103486
907	8807	150071	192147	82155	2607	112580
953	8237	95016	117410	86101	2565	111579
967	8243	58601	118078	86966	3016	152838
971	9551	95634	145776	93232	2804	139996
977	7817	56356	114479	87090	2707	110835
991	9349	65892	137322	89147	2731	271611
997	5393	42634	86518	91078	2883	85876
1013	7177	53302	109643	89958	2765	109649
1019	6691	48599	102173	90620	2831	101650
1021	8819	59581	131857	92489	2716	131150

Таблиця 2

Результати досліджень відносно оптимізації множення поліномів для NTRU методу з модифікованими параметрами

p	*q*	**Показники швидкодії шифрування у тактах процесора**			**Показники швидкодії шифрування**		
		KeyGen	**Encrypt**	**Decrypt**	**KeyGen, ms**	**Encrypt, Mbit/s**	**Decrypt, Mbit/s**
673	9413	81137116	236834	124986	26.8216	10.5313	19.3952
691	6449	79746185	209416	103788	26.6518	12.4174	23.9656
719	9133	89988642	242626	127904	29.7004	11.0166	19.4711
727	5827	87258688	192654	96051	28.4078	13.9774	26.3697
739	9829	94319308	270423	139869	31.1194	10.0539	19.8775
743	7541	92670350	222166	123160	30.98	12.5694	22.453
757	7879	96724781	231926	125563	32.0007	12.2059	22.6533
761	7883	97740894	233048	122197	31.9362	12.2551	22.0994
769	6599	97128257	211943	106017	32.2375	13.6429	25.87
773	9811	100393573	269918	140504	33.4946	10.9252	20.3127
787	4243	98758503	178990	89072	32.64	16.5373	32.6901
809	6113	104344176	213954	108083	34.8262	14.1635	26.3957
811	8543	108552086	255410	132414	35.5397	11.9486	22.6838
823	8069	111309145	256163	128736	36.9474	12.5428	23.973
827	9767	112265692	277923	147490	37.7937	11.2176	19.5569
853	9721	119377243	284659	148806	39.3514	11.3944	21.5935
857	5167	116551976	208268	99091	38.5389	15.6327	30.8011
863	8779	119387521	278985	139606	39.8311	12.1471	23.2145
881	3217	118593929	182071	83380	38.923	18.541	39.8288
941	2521	131344006	175659	74479	43.4393	20.4683	47.666
947	3917	136057581	203357	97532	45.0785	18.1485	36.8701
1009	4259	151405035	220684	105639	50.7393	17.8264	36.6911
1013	3923	153522542	214756	106304	51.2598	18.3456	36.6911
83	8089	124938084	262572	135157	42.0974	12.216	23.3983
907	8807	129346765	279548	143837	43.5581	11.7818	22.7099
953	8237	142236375	281616	146901	47.105	12.4677	23.2038
967	8243	145962556	281165	150954	48.6366	11.801	23.2006
971	9551	147677455	305294	168921	49.5779	11.2187	20.0617
977	7817	149305234	283842	146744	49.6083	12.9946	24.1718
991	9349	151407064	307350	174862	51.3147	11.8333	21.1004
997	5393	150358985	237968	119046	50.1645	15.2628	30.394
1013	7177	157913719	273759	144236	52.8602	13.6686	24.9641
1019	6691	159746211	266936	138704	53.1059	14.0228	26.7991
1021	8819	160598240	318723	165008	53.1704	11.6696	22.7558

Слід звернути увагу, що швидкісні показники операції зашифрування для модифікованого методу є прогнозовано слабкішими за опера-

цію розшифрування (див. табл. 1). Так, з табл. 1 видно, що значну кількість часу відводиться на обчислення сліпого поліному r, перетворення до рядку байтів (ToBytes) при зашифруванні також займає час на порядок більший за зворотне перетворення до поліному (ToPol) при розшифруванні. При цьому швидкісні показники множення поліномів (Mul), які займають значну кількість часу відносно виконання усього алгоритму, є приблизно однаковими в операціях шифрування.

Швидкісні показники операції множення поліномів, одержані за рахунок проведення оптимізації обчислень. Самі поліноми задаються номерами ненульових коефіцієнтів, що дозволило зменшити число повторень циклів. Для накопичення суми при обчисленні коефіцієнтів результуючого полінома використовувалися AVX операції, це дозволило одночасно накопичувати 8 коефіцієнтів. Для обчислення модуля по поліному використовувалася операція додавання замість операції ділення. Поки не вдалося оптимізувати обчислення модуля по простому числу q.

При обчисленні сліпого поліному r основний час займає многократна операція гешування для формування випадкових коефіцієнтів полінома і обчислення самих коефіцієнтів. З метою оптимізації при обчисленні геш значення використовувалися попередні обчислювання і AVX операції. Поки не вдалося оптимізувати визначення самих коефіцієнтів полінома. Залежно від випадкового компонента операцію шифрування фактично іноді доводиться виконувати повторно. Що істотно збільшує час операції шифрування.

Одержані результати відносно швидкодії для NTRU методу зі модифікованими параметрами порівнювалися зі швидкісними показниками реалізації NTRU методу зі стандартизованими параметрами, наданими в ресурсі [4], результати, для відповідного набору параметрів були зведені у табл. 3.

Таблиця 3

Порівняння результатів швидкодії NTRU методу класичного і з модифікованими параметрами

NTRU метод	p	q	**Показники швидкодії у тактах процесора**		**Характеристика процесора**
			Зашифрування	**Розшифрування**	
ntruees743ep1 [4]	743	2048	101626	109118	Intel (R) Core (TM) i5 - 6600 CPU @ 3.31 GHz
модифікований	659	7481	214428	101148	Intel (R) Core (TM) i5 - 4440 CPU @ 3.10 GHz

Висновки. Ми дослідили можливість використання нового класу параметрів для алгоритму [1] та часові характеристики для усіх сто двадцяти двох параметрів зі роботи [2]. При реалізації використову-

валась алгоритмічна оптимізація та оптимізація за рахунок властивостей сучасних процесорів. Особлива увага надана функції множення поліномів, яка займає приблизно половину часу виконання операцій зашифрування та розшифрування (співвідношення залежить від кількості ненульових елементів). Використання AVX команд та грамотне застосування властивостей кешу також дозволило суттєво вплинути на час виконання операцій.

Отриманий результат показав, що зменшення продуктивності за рахунок використання нових параметрів не перевищує 50%, що, на наш погляд, є допустимим.

У подальшому планується покращити показники швидкодії, наприклад, за рахунок оптимізації обчислення модуля по простому числу q та оптимізації визначення коефіцієнтів полінома, зменшивши тим самим час шифрування та розшифрування.

Список використаних джерел:

1. American National Standard X9.98-2010. Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment: Part 2: Data Encryption, 2010. Lattice-Based Polynomial Public Key Establishment Algorithm for the Financial Services Industry.
2. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal. NTRU Prime [Електронний ресурс]. Режим доступу: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf (visited 22.12.2016).
3. Post-Quantum crypto Project [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-crypto/rfc-july2016.html.
4. Measurements of public-key cryptosystems, indexed by machine [Електронний ресурс]. Режим доступу: https://bench.cr.yp.to/ results-encrypt.html.

Researched a new class of parameters such NTRU algorithm optimized basic algorithmic operations.

Key words: *NTRU similar algorithms, computational complexity, time productivity.*

Одержано 01.03.2017