10. Малачівський П. С., Пізюр Я. В. Розв'язування задач в середовищі Maple. Львів : Видавництво «РАСТР–7». 2016. 282 с.

CHEBYSHEV APPROXIMATION BY RATIONAL EXPRESSION FUNCTIONS OF TWO VARIABLES

The method for constructing of Chebyshev approximation by rational expression for function of two variables is proposed. Idea of the method is based on constructing the boundary power-average approximation in L^p norm with $p \to \infty$. Least square method with two weight functions is used to construct of this approximation. One weight function ensures the construction of power-average approximation, and another refines parameters of rational expression by linearization scheme. Iterative refinement of weight functions values is proposed. Results of test examples solving confirm the effectivity of proposed method.

Key words: *Chebyshev approximation by rational expression, function of two variables, power-average approximation, least square method.*

Одержано 31.01.2019

УДК 621.391:519.2
DOI: 10.32626/2308-5916.2019-19.81-87

А. А. Матійко

Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ NTRUENCRYPT ТА NTRUCIPHER

Асиметрична система шифрування NTRUEncrypt запропонована в 1996 р. та є однією з найшвидших постквантових шифросистем. Вона включена до стандарту ANSI X9.98-2010 та є прототипом широкого класу криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів в деяких решітках. Криптографічні властивості шифросистеми NTRUEncrypt достатньо повно досліджені, а її останні модифікації представлено на поточному конкурсі NIST із стандартизації постквантових асиметричних алгоритмів шифрування, інкапсуляції ключів та цифрового підпису.

Однією з актуальних задач у галузі криптології є створення симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї конкретної задачі (наприклад, для RSA це — задача факторизації чисел). У зв'язку з цим в 2017 р. на базі NTRUEncrypt запропонована симетрична шифросистема NTRUCipher, для якої проведено попередній аналіз стійкості та запропоновано алгоритм вибору парамет-

рів. Поряд з тим, у доведенні CPA-стійкості алгоритму шифрування NTRUCipher містяться суттєві помилки; до того ж залишається не вирішеною задача порівняльного аналізу шифросистем NTRUCipher та NTRUEncrypt за стійкістю та практичністю.

Мета цієї роботи — проведення порівняльного аналізу зазначених шифросистем, а також коректне обґрунтування умов, що забезпечують CPA-стійкість шифросистеми NTRUCipher. Окремим результатом є аналітичні оцінки ймовірності помилкового розшифрування повідомлень для NTRUCipher, що є важливим для належного вибору параметрів шифросистеми при її практичному застосуванні. Показано, що значення ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUCipher змінюється в межах від 2^{-357} до 2^{-157} водночас як значення цієї ймовірності для шифросистеми NTRUEncrypt змінюється в межах від 2^{-160} до 2^{-74}. Крім того, отримані оцінки не базуються на жодних евристичних припущеннях.

Ключові слова: *постквантова криптографія, NTRUEncrypt, NTRUCipher, ймовірність помилкового розшифрування, CPA-стійкість.*

Вступ. Однією з актуальних задач у галузі криптології є створення симетричних шифросистем, стійкість яких базується на складності розв'язанні лише однієї конкретної обчислювальної задачі. Прикладом такої шифросистеми є NTRUCipher [1], що являє собою симетричний аналог відомої асиметричної шифросистеми NTRUEncrypt [2]. Попередній аналіз стійкості NTRUCipher, проведений в [1], містить суттєві помилки. Крім того, залишається не вирішеною задача порівняльного аналізу шифросистем NTRUCipher та NTRUEncrypt за стійкістю та практичністю.

Мета роботи — проведення порівняльного аналізу зазначених шифросистем, а також коректне обґрунтування умов, що забезпечують CPA-стійкість шифросистеми NTRUCipher. Окремим результатом є аналітичні оцінки ймовірності помилкового розшифрування повідомлень для NTRUCipher, які не базуються на жодних евристичних припущеннях.

Означення основних понять та загальний опис шифросистем. Нехай n та q — взаємно прості натуральні числа, $n, q > 3$, q не ділиться на 3. Позначимо Z_q кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$ для непарного q та інтервалу $[-q/2, q/2-1]$ для парного q. Позначимо $R_{n,q} = Z_q[x]/(x^n - 1)$ — кільце зрізаних поліно-

мів степеня не вище n над кільцем Z_q, $R^*_{n,q}$ — множину оборотних елементів кільця $R_{n,q}$.

Нехай S — множина всіх малих поліномів (коефіцієнти яких належать множині $\{-1, 0, 1\}$) степеня не вище n, S_e — певна фіксована підмножина множини S. Для будь-яких натуральних чисел d_1, d_2 позначимо S_{d_1,d_2} — множину всіх малих поліномів степеня не вище n, серед коефіцієнтів яких є точно d_1, що дорівнюють 1, та точно d_2, що дорівнюють -1.

В табл. 1 наведено означення шифросистем NTRUCipher [1] та NTRUEncrypt [2]. Як видно з таблиці, обидві шифросистеми мають схожу будову. При цьому в NTRUCipher використовується тільки секретний ключ, що є у два рази коротше секретного ключа шифросистеми NTRUEncrypt. Отже, основними критеріями, за якими проведено порівняльний аналіз зазначених шифросистем, є:

1) малість ймовірності помилкового розшифрування повідомлень [3, 4];
2) умови стійкості відносно атак на основі підібраних відкритих повідомлень (CPA-стійкості) [5].

Таблиця 1

Опис шифросистем NTRUEncrypt та NTRUCipher

NTRUEncrypt	**NTRUCipher**
асиметричний алгоритм шифрування	симетричний алгоритм шифрування
секретний ключ: (F, g), де $F \in S_{d,d}$ є таким, що $f = 1 + 3F \in R^*_{n,q}$; $g \in S_{d'+1,d}$', де $d' = \lfloor n/3 \rfloor$	секретний ключ: $F \in S_{d,d}$ є таким, що $f = 1 + 3F \in R^*_{n,q}$
відкритий ключ: $h = 3g / f$ (обчислюється в кільці $R^*_{n,q}$)	—
алгоритм зашифровування: $\mathrm{E}_h(m, r) = (m + rh + 3e) \bmod q$, де $m \in S$ — відкритий текст, $r \in S_{d,d}$ та $e \in S_e$ — незалежні випадкові поліноми	алгоритм зашифровування: $\mathrm{E}_h(m, r) = (m + 3r / f + 3e) \bmod q$, де $m \in S$ — відкритий текст, $r \in S_{d,d}$ та $e \in S_e$ — незалежні випадкові поліноми
алгоритм розшифровування: $D_f(c) = cf \pmod q \bmod 3$, де $c \in R_{n,q}$ — шифротекст	алгоритм розшифровування: $D_f(c) = cf \pmod q \bmod 3$, де $c \in R_{n,q}$ — шифротекст

Враховуючи обмеження щодо обсягу статті, доведення отриманих тверджень не наводяться.

Ймовірність помилкового розшифрування повідомлень. В роботі [4] для NTRUEncrypt отримано оцінку ймовірності $p_{er}(F,g) = \mathrm{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ за умови, що $S_e = \{0\}$, поліноми $F \in S_{d,d}$ і $g \in S_{d'+1,d}$ є фіксованими, а коефіцієнти поліномів m, r є незалежними випадковими величинами, розподіленими за законами

$$\mathrm{P}(g_i = 1) = \mathrm{P}(g_i = -1) = d'n^{-1},\ \mathrm{P}(g_i = 0) = 1 - 2d'n^{-1},$$

$$\mathrm{P}(m_i = 1) = \mathrm{P}(m_i = -1) = \mathrm{P}(m_i = 0) = 1/3, \quad (1)$$

$$\mathrm{P}(r_i = 1) = \mathrm{P}(r_i = -1) = dn^{-1},\ \mathrm{P}(r_i = 0) = 1 - 2dn^{-1}; \quad (2)$$

$$p_{er}(F,g) \le 2n \exp\{-\frac{(q-2)^2}{72(2d+2d'+1)}\}. \quad (3)$$

Для шифросистеми NTRUCipher має місце таке твердження.

Твердження 1. Нехай $F \in S_{d,d}$, $S_e = \{0\}$, а коефіцієнти поліномів m і r є незалежними випадковими величинами, розподіленими за законами (1) і (2) відповідно. Тоді для ймовірності $p_{er}(F) = \mathrm{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ справедлива нерівність

$$p_{er}(F) \le 2n \exp\{-\frac{(q-8)^2}{72(2d+1)}\}. \quad (4)$$

В табл. 2 для низки пар (n,d), перші п'ять з яких рекомендовано в [6], а дві останні — в [3], наведені значення $-\log_2 p_{er}$ для шифросистем NTRUEncrypt та NTRUCipher; при цьому $q = 2048$.

Таблиця 2

Результати оцінювання параметрів, що характеризують частоту виникнення помилок розшифрування

(n,d)	$-\log_2 p_{er}$ (NTRUEncrypt)	$-\log_2 p_{er}$ (NTRUCipher)
(401, 113)	160,49	357,69
(449, 134)	138,12	300,18
(677, 157)	99,24	254,32
(1087, 120)	75,84	334,92
(1171, 106)	73,28	380,29
(443, 143)	134,58	280,76
(743, 247)	74,28	157,92

Як видно з даної таблиці, значення ймовірності помилкового розшифрування повідомлень шифросистеми NTRUCipher на декілька

порядків нижча і змінюється в межах від 2^{-357} до 2^{-157} водночас, коли значення цієї ймовірності для шифросистеми NTRUEncrypt змінюється в межах від 2^{-160} до 2^{-74}. При $(n,d)=(401,113)$ в обох шифросистемах спостерігається найменша ймовірність виникнення помилок розшифрування повідомлень.

Умови CPA-стійкості шифросистем. Нагадаємо відоме означення CPA-стійкості симетричної шифросистеми (див., наприклад, [5]). Розглядається така «гра» між противником і дослідником:

1) дослідник генерує секретний ключ k;
2) противник може подавати на вхід оракула E_k, що здійснює зашифрування, будь-які відкриті та отримувати відповідні шифровані повідомлення;
3) противник подає дослідникові пару різних повідомлень m_0 та m_1 однакової довжини;
4) дослідник вибирає випадкове рівноймовірне число $b \in \{0,1\}$ та повертає противнику шифроване повідомлення $c = E_k(m_b)$;
5) противник може звертатися до оракула E_k (як в п. 2)) і повинен відновити значення b.

Шифросистема називається (T,ε)-CPA-стійкою, якщо будь-який алгоритм відновлення значення b з імовірністю $\varepsilon > 1/2$ у наведеній «грі» виконує не менше ніж T операцій. CPA-стійкість асиметричних шифросистем визначається аналогічним чином.

Відомі наступні обчислювально складні задачі, пов'язані з NTRU-подібними шифросистемами [7].

Задача 1 (NTRU Decision Key Craking Problem) полягає у встановленні закону розподілу випадкового елемента h, який з імовірністю $1/2$:

- має рівномірний розподіл на множині $R_{n,q}$ (гіпотеза H_0);
- формується за правилом $h = 3r/f$, де r і f є незалежними випадковими елементами з рівно ймовірним розподілом на множинах S і $S_{d,d} \cap R^*_{n,q}$ відповідно (гіпотеза H_1).

Задача 2 (NTRU Search Key Craking Problem) полягає у тому, щоби для заданої множини $S_e \subseteq S$ та згенерованого випадкового рівноймовірного елемента $h \in R_{n,q}$ встановити закону розподілу випадкового елемента c, який з імовірністю $1/2$:

- має рівномірний розподіл на множині $R_{n,q}$ (гіпотеза H_0);
- формується за правилом $c = 3(hr + e)$, де r і e є незалежними випадковими елементами з рівноймовірним розподілом на множинах S і S_e відповідно (гіпотеза H_1).

Відомо [7], що шифросистема NTRUEncrypt

- є CPA-стійкою лише за умови, що обидві задачі (1 і 2) є обчислювально складними;
- може не бути CPA-стійкою, якщо задача 2 не є обчислювально складною (наприклад, коли $S_e = \{0\}$).

Другим результатом цієї статті є наступне твердження.

Твердження 2. Нехай існує CP-атака на NTRUCipher зі складністю T та ймовірністю успіху $\varepsilon > 1/2$. Тоді існує алгоритм розв'язання Задачі 1 зі складністю $T + c$ та ймовірністю успіху $1/2 \cdot (1 + \varepsilon)$, $c = \text{const}$. Іншими словами, шифросистема NTRUCipher є CPA-стійкою за умови високої обчислювальної складності лише задачі 1.

Висновки. Симетрична система шифрування NTRUCipher будується подібно до її асиметричного аналога NTRUEncrypt, але використовує секретний ключ, що має вдвічі меншу довжину. Значення ймовірності помилкового розшифрування повідомлень в NTRUCipher є на декілька порядків нижче і змінюється в межах від 2^{-357} до 2^{-157} водночас, як значення цієї ймовірності для NTRUEncrypt змінюється в межах від 2^{-160} до 2^{-74}. Крім того, шифросистема NTRUCipher є CPA-стійкою за більш слабких умов в порівнянні з NTRUEncrypt. Для забезпечення стійкості першої шифросистеми достатньо лише високої обчислювальної складності задачі 1, в той час як друга шифросистем є стійкою за умови високої складності обох задач 1 і 2 (і може бути не стійкою у протилежному випадку).

Список використаних джерел:

1. Valluri M. R. NTRUCipher-lattice based secret key encryption. arXiv: 1710.01928V2. 6/10/2017
2. Hoffstein J., Pipher J., Silverman J.H. NTRU: a new high speed public key cryptosystem. Preprint, presented at the rump session of Crypto'96. 1996.
3. Hirschhorn P., Hoffstein J., Howgrave-Graham N., Whyte W. Choosing NTRU parameters in light of combined lattice reduction and MITM aproaches. Applied Cryptography and Network Security, LNCS. 2009. Vol. 5536. P. 437–455.
4. Олексійчук А. М., Матійко А. А. Оцінки ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUEncrypt при фіксованому ключі. *Захист інформації.* 2018. № 2. С. 89–94.
5. Katz J., Lindell Y. Introduction to modern cryptography. CRC Press, 2015.

6. Chen C., Hoffstein J., Whyte W., Zhang Z. NIST PQ Submission: NTRUEncrypt. A lattice based algorithm. URL: https://cscr.nist.gov/Projects/-Post-Quantum-Cryptorraphy, 2017.
7. Steinfeld R. NTRU cryptosystem: resent developments and emerging mathematical problems in finite polynomial rings. URL: http://users.monach.edu.au/-~rste /NTRU_survey.pdf. 2014.

THE COMPARATIVE ANALYSIS OF NTRUCIPHER AND NTRUENCRYPT ENCRYPTION SCHEMES

The asymmetric encryption scheme NTRUEncrypt proposed in 1996 and is one of the fastest post-quantum encryption schemes. It is included in the ANSI X9.98-2010 standard and is the prototype of cryptosystems' wide class with the same name, which security is based on the difficulty of finding short vectors in some lattices. The cryptographic properties of NTRUEncrypt encryption scheme are sufficiently explored and its latest modifications are presented at the current NIST competition to standardize post-quantum asymmetric encryption, key encapsulation and digital signature.

One of the most important problem in the field of cryptology is the design of symmetric encryption schemes, whose security, similarly to the asymmetric one, is based on the complexity of solving only one particular problem (for example, for RSA this is the problem of factorization of numbers). Due to this, in 2017 the symmetric encryption scheme NTRUCipher based on NTRUEncrypt was proposed. For it, a preliminary security analysis was performed and a parameter selection algorithm was proposed. At the same time, there are essential errors in the proof of CPA-security of the encryption algorithm NTRUCipher. Moreover, the problem of comparative analysis of NTRUCipher and NTRUEncrypt encryption schemes is not solved for security and practicality.

The purpose of this article is to conduct a comparative analysis of the abovementioned encryption schemes and to prove correctly the conditions that ensure the CPA-security of the NTRUCipher encryption scheme. A certain result is analytical bounds of decryption failure probability in NTRUCipher encryption scheme. This result is important for the proper parameters' choice of the encryption scheme in its practical implementation. It is shown that the decryption failure probability in the NTRUCipher varies from 2^{-357} to 2^{-157} while the value of this probability for the NTRUEncrypt encryption scheme varies from 2^{-160} to 2^{-74}. In addition, the obtained bounds are not based on any heuristic assumptions.

Key words: *post-quantum cryptography, NTRUEncrypt, NTRUCipher, decryption failure probability, CPA-security.*

Одержано 21.01.2019