УДК 519.2

А.М. ОЛЕКСІЙЧУК
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alex-dtn@ukr.net*.

А.А. МАТІЙКО
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *alexm1710@ukr.net*.

РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher

Анотація. Запропоновано розрізнювальну атаку на симетричну шифросистему NTRUCipher, визначену над кільцем лишків за модулем циклотомічного полінома над скінченним полем простого порядку. Атака базується на існуванні гомоморфізму цього кільця у зазначене поле та може бути досить ефективною за достатньо загальних умов.

Ключові слова: решіткова криптографія, симетрична шифросистема, розрізнювальна атака, циклотомічний поліном, NTRUCipher.

Шифросистему NTRUCipher запропоновано в роботі [1] як симетричний аналог відомої асиметричної схеми шифрування NTRUEncrypt [2]. У працях [3, 4] досліджено різні версії цієї шифросистеми та описано низку атак на них.

У цій статті запропонована розрізнювальна атака (distinguishing attack) на оригінальну версію шифросистеми NTRUCipher [1], яка визначається над кільцем $R(n, q) = \mathbf{Z}_q[x] / (x^n + 1)$, де $n \geq 2$ — степінь двійки, а q – просте число таке, що $q \equiv 1 \bmod 2n$. Ця атака базується на існуванні гомоморфізму кільця $R(n, q)$ у поле $\mathbf{Z}_q$ та, як показано далі, може бути ефективною за достатньо загальних обмежень.

Зауважимо, що за умови $q \equiv 1 \bmod 2n$ мультиплікативна група поля $\mathbf{Z}_q$ містить циклічну підгрупу порядку $2n$, і якщо β є твірним елементом цієї підгрупи, то поліном $x^n + 1$ розкладається над полем $\mathbf{Z}_q$ на лінійні співмножники: $x^n + 1 = (x - \beta)(x - \beta^3) \cdots (x - \beta^{2n-1})$, а отже, збігається з $2n$-циклотомічним поліномом над цим полем (див., наприклад, [5, означення 2.44]).

Зауважимо також, що кільце $R(n, q)$ часто використовується для побудови асиметричних NTRU-подібних (та близьких до них) шифросистем (див., наприклад, [6, 7]). Це пояснюється можливістю застосування швидкого перетворювання Фур'є над полем $\mathbf{Z}_q$ для множення елементів кільця $R(n, q)$, а також відомим результатом [8] стосовно складнісної еквівалентності двох версій задачі Ring-LWE над цим кільцем, що важливо для доведення стійкості (security proof) відповідних криптосистем.

Шифросистема NTRUCipher над кільцем $R(n, q)$ визначається таким чином. Для зашифрування відкритого тексту $m \in R(n, q)$, який є поліномом з коефіцієнтами $0, 1, -1$, на секретному ключі f, що вибирається у визначений спосіб з групи $R(n, q)^*$ оборотних елементів кільця $R(n, q)$, генерується випадковий поліном $r \in R(n, q)$ та обчислюється шифрований текст $c = (m + 3rf^{-1}) \bmod q$. Розшиф-