Про неіснування матриць максимального індексу розгалуження над кільцем лишків за модулем 2^n

С.В. Яковлєв
кафедра математичних методів захисту інформації,
Фізико-технічний інститут,
Національний технічний університет Україні
«Київський політехнічний інститут»,
Київ, Україна
yasv@rl.kiev.ua

В.В. Дідан
кафедра математичних методів захисту інформації,
Фізико-технічний інститут,
Національний технічний університет Україні
«Київський політехнічний інститут»,
Київ, Україна
vdidan@mail.ru

On the non-existence of matrices of maximum branch number over ring of residues modulo 2^n

S. Yakovlev
Department of Mathematical Methods of Information Security,
Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
Kyiv, Ukraine
yasv@rl.kiev.ua

V. Didan
Department of Mathematical Methods of Information Security,
Institute of Physics and Technology,
National Technical University of Ukraine
"Kyiv Polytechnic Institute"
Kyiv, Ukraine
vdidan@mail.ru

***Анотація* — Доведено неіснування матриць максимального індексу розгалуження над кільцем лишків за модулем 2^n та проаналізовано наслідки для побудови криптографічних алгоритмів, які використовують операцію додавання за модулем для лінійного розсіювання.**

***Abstract* — We prove that no matrix over the ring of residues modulo 2^n has maximal branch number and show how this claim influences the cryptographic properties of algorithms which uses modular addition in the linear diffusion layer.**

Ключові слова — індекс розгалуження; розсіюючий шар; додавання за модулем

Keywords — branch number; diffusion layer; modular addition

I. Вступ

Всі сучасні симетричні блокові шифри побудовані відповідно до класичних принципів Шеннона [1] і складаються з лінійних перетворень, які забезпечують розсіювання статистичних характеристик (diffusion), та нелінійних перетворень, які забезпечують перемішування (confusion) даних та ключа. Розсіюючий шар виконує істотну роль в блокових шифрах. Він забезпечує стійкість проти таких відомих атак на блокові шифри, як диференціальний та лінійний криптоаналіз [2, 3].

Одним з найбільш популярних типів лінійних перетворень, що використовуються блокових шифрах, є перетворення на основі матриць з максимальним індексом розгалуження над скінченим полем характеристики 2. Шари такого типу використовуються в таких відомих блокових шифрах, як AES [4], «Кузнєчік» [5], ДСТУ 7624:2004 («Калина») [6].

На даний момент перетворення над скінченними полями характеристики 2, які використовуються в блокових шифрах, достатньо вивчені, обґрунтований їх вплив на стійкість шифру до різного роду атак, чого не можна сказати про перетворення над кільцем лишків за модулем. Однак операція додавання за модулем має ряд бажаних криптографічних властивостей, зокрема, суттєво підвищує стійкість шифрів до лінійного та алгебраїчного криптоаналізу. Тому постає задача пошуку перетворень над кільцем лишків за модулем 2^n, використання яких дало б змогу побудувати криптографічно стійкі шифри з теоретичної та практичної точки зору.

Поставлене завдання вирішується шляхом побудови перетворення над кільцем лишків аналогічно

перетворенню над скінченим полем, а саме: побудова матриці максимального індексу розгалуження над кільцем лишків за модулем 2^n.

II. Необхідні терміни та позначення

Кільце лишків за модулем 2^n – це алгебраїчна структура, що складається з множини цілих чисел від 0 до 2^n-1 та визначеними на ній операціями додавання та множення за модулем 2^n.

Матриця $m\times n$ над кільцем лишків за модулем 2^n – це прямокутна таблиця $A=\|a_{ij}\|$, $1\le i\le m$, $1\le j\le n$, де кожен a_{ij} є елементом кільця лишків за модулем 2^n.

Підматрицею матриці A називається матриця, що отримана шляхом викреслювання рядків або стовпців матриці A.

Матриця над кільцем лишків за модулем 2^n є невиродженою, якщо її визначник взаємнопростий з 2^n, тобто є непарним числом.

Індексом розгалуження β матриці M розмірності $k\times k$ над кільцем лишків за модулем 2^n називається найменше число з суми ненульових елементів $k\times 1$-вектора X та $k\times 1$-вектора $Y=M\cdot X$ (позначається як $wt(X)$ і $wt(Y)$ відповідно) серед всіх $X\neq 0$, тобто $\beta=\min\limits_{X\neq 0}\{wt(X)+wt(Y)\}$, де $X=(x_1,x_2,...,x_k)^T$ та $Y=(y_1,y_2,...,y_k)^T$ – вектори, що складаються з елементів кільця лишків за модулем 2^n.

Індекс розгалуження β називається максимальним, якщо для матриці M розмірності $k\times k$ він дорівнює $k+1$ [7].

III. Пошук Матриць з Максимальним Індексом Розгалуження над Кільцем Лишків за Модулем 2^N

Для матриці M розмірності $n\times n$ доведено [8], що $\beta=n+1$ тоді і тільки тоді, коли ранг кожної підматриці матриці M розмірності $k\times k$ дорівнює k для всіх $1\le k\le n$, тобто всі квадратні підматриці є невиродженими. Перевіримо, чи виконується дана умова для матриць над кільцем лишків за модулем 2^n.

Нехай M – матриця розмірності $n\times n$ над кільцем лишків за модулем 2^n, β – індекс розгалуження матриці M. Нехай для $n\times 1$-вектора X маємо $wt(X)=l$. Тоді для вектора $Y=M\cdot X$ справедливо $wt(Y)\ge\beta-l$ за визначенням індексу розгалуження. Розглянемо вектори X з одним ненульовим елементом, тобто $wt(X)=1$. Тоді щоб індекс розгалуження для матриці M був максимальним необхідно, щоб $wt(Y)=n$. Але якщо відповідний стовпчик матриці M містить парні елементи, то для них можна підібрати такі множники, які дадуть у результуючому векторі Y нульове значення у відповідній координаті. Таким чином, для того, щоб індекс розгалуження був максимальним, необхідно, що матриця M складалась лише з непарних елементів.

Розглянемо тепер довільну підматрицю розмірності 2×2 матриці . Очевидно, що оскільки всі її елементи – непарні числа, то її визначник буде парним числом. Отже, всі ці підматриці є виродженими над кільцем лишків за модулем 2^n, що суперечить умові. Таким чином, над кільцем лишків за модулем 2^n не існує матриць з максимальним індексом розгалуження.

IV. Висновки

Індекс розгалуження є важливим параметром лінійних перетворень, які використовуються у слово-орієнтованих симетричних шифрах та геш-функціях. Чим більше значення індексу розгалуження, тим вища стійкість відповідного криптоалгоритму до диференціальних та лінійних атак. Операція модульного додавання також має добрі криптографічні властивості, що підвищує стійкість криптографічних алгоритмів до лінійних та алгебраїчних атак. Однак в даній роботі було показано, що ці дві властивості в деякому сенсі суперечать одна одній, оскільки лінійні перетворення над кільцем лишків за модулем 2^n принципово не можуть досягнути максимального значення індексу розгалуження.

При побудові криптографічних примітивів певного рівня стійкості необхідно враховувати цей факт та підвищувати стійкість до відомих криптографічних атак не тільки за рахунок лінійного розсіюючого шару, але й іншими засобами. В подальших дослідженнях планується знайти максимальне теоретичне значення індексу розгалуження матриць над кільцем лишків та побудувати перетворення, застосовні з криптографічної точки зору.

V. Література References

[1] C. E. Shannon, “Communication theory of secrecy systems”, Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949.

[2] E. Biham, A. Shamir, “Differential Cryptanalysis of DES-Like Cryptosystems”, CRYPTO ’90, LNCS, vol. 537, pp. 2-21, Springer, 1991.

[3] M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, EUROCRYPT ’93, LNCS, vol. 765, pp. 386-397, Springer, 1994.

[4] J. Daemen, V. Rijmen, “The design of Rijndael: AES – The Advanced Encryption Standard”, Springer Verlag , 2002.

[5] Shishkin, V. Low-Weight and Hi-End: Draft Russian Encryption Standard. / V. Shishkin, D. Dygin, I. Lavrikov, G. Marshalko, V. Rudskoy, and D. Trifonov // Current Trends in Cryptology (Moscow, 2014). — 2014. — pp. 183—188.

[6] Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.

[7] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, Hamidreza Maimani, Einollah Pasha, “Construction of New Families of MDS Diffusion Layers”, IACR Cryptology ePrint Archive, 2014 [Online]. Available: https://eprint.iacr.org/2014/011.

[8] Ju-Sung Kang et al, “Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks”, ETRI Journal, Vol.23, No.4, Dec. 2001.