УДК 003.26:519.21+512.624

ЦІЛКОМ АФІННА ЕКВІВАЛЕНТНІСТЬ ЕКСПОНЕНЦІЙНИХ S-БЛОКІВ

Я. В. Кратт[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі запропоновано новий тип афінної еквівалентності, специфічний для експоненційних перетворень у скінченних полях характеристики 2. Використання запропонованого типу еквівалентності дозволяє розширити множину застосовних у криптографічних цілях S-блоків на основі експоненційних перетворень, оскільки при цьому зберігаються притаманні експоненційним S-блокам криптографічні властивості.

Ключові слова: експоненційні S-блоки, афінна еквівалентність S-блоків, EA-еквівалентність S-блоків

Вступ

Криптографічна стійкість шифрів значною мірою визначається їх нелінійними елементами, зокрема, S-блоками. Вибір S-блоків для алгоритмів блокового шифрування безпосередньо впливає на стійкість до лінійного та диференціального криптоаналізу, а також алгебраїчних атак. Серед перспективних методів побудови криптографічних S-блоків можна виокремити метод на основі експоненційних перетворень у скінченних полях, запропонований Сергієм Агієвичем та Андрієм Афоненком; у роботі [1] ці дослідники формулюють достатні критерії для забезпечення ряду криптографічних властивостей експоненційних S-блоків.

У даній роботі розглядаються бієктивні експоненційні S-блоки фіксованого розміру. Буде запропоновано та проаналізовано новий тип афінної еквівалентності, специфічний саме для експоненційних перетворень у скінченних полях характеристики 2, який дозволяє, з одного боку, суттєво розширити множину S-блоків, а з іншого – забезпечує зберігання притаманних експоненційним перетворенням криптографічних властивостей.

1. Основні терміни та означення

Нехай $\mathbb{F}_{2^n}$ – скінченне поле, елементи якого мають представлення як бітові вектори: $x = (x_0, \dots, x_{n-1}) \in \mathbb{F}_{2^n}$. *Експоненційне відображення над полем* $\mathbb{F}_{2^n}$ [1] – це відображення виду

$$s : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}, \quad s(x) = \begin{cases} 0, & x = 0 \\ \alpha^{\overline{x}}, & x = 0, \end{cases}$$

де $\overline{x} = x_0 + 2 \cdot x_1 + ... + 2^{n-1} \cdot x_{n-1}$ – число, двійковим представленням якого виступає вектор $x = (x_0, x_1, \cdots, x_{n-1})$, $\alpha \in \mathbb{F}_{2^n}^*$ — примітивний елемент мультиплікативної групи поля. Зауважимо, що примітивність елементу α необхідна та достатня для бієктивності введеного експоненційного відображення.

Агієвич та Афоненко встановили [1], що експоненційні відображення при виконанні певних додаткових умов задовольняють низці криптографічних характеристик, зокрема:

- досягаються мінімальні значення $(+, \oplus)$-диференціальних імовірностей: за відомою різницею між прообразами x_1 і x_2 (відносно модульного додавання) імовірність одержати наперед задану різницю між образами $s(x_1)$ і $s(x_2)$ (відносно побітового додавання) не перевищує $4 \cdot 2^{-n}$, а при деяких додаткових обмеженнях – $3 \cdot 2^{-n}$;
- висока алгебраїчна нелінійність: довільна лінійна комбінація координатних функцій $s(x)$ має майже максимальний алгебраїчний степінь;
- досягається істотне поширення помилок (лавинні ефекти): зміна значення однієї або декількох координат вхідного вектору x призводить до зміни кожної з координат виходу $s(x)$ з ймовірністю, близькою до $1/2$.

Нехай V_n – множина усіх n-бітових векторів. Дві булеві функції $F, G \colon V_n \to V_n$ є *розширено афінно еквівалентними (EA-еквівалентними)*[2], якщо існують афінні бієктивні функції A_1, A_2 та деяка афінна функція A такі, що виконується

$$F(x) = A_2(G(A_1(x))) \oplus A(x).$$

Для звичайних (багатовимірних) булевих функцій розглядаються афінні перетворення виду $A(x) = L \cdot x \oplus b$, де L – (невироджена) двійкова матриця, x та b – двійкові вектори відповідного розміру.

2. Цілком афінна еквівалентність експоненційних S-блоків

Для спрощення викладення будемо записувати експоненційні S-блоки як

$$s(x) = a^x, \text{ де } x \in \mathbb{Z}_{2^n},\ s(x) \in \mathbb{F}_{2^n}.$$

Зауважимо, що $s(0) = 0$, в той час як $a^0 = 1$ (і значення $s(x) = 1$ досягається також при $x = 2^n - 1$). Втім,

у тих випадках, коли мова буде йти про значення експоненційного S-блоку у точці 0, ми будемо вважати $a^0 = 0$, а під час певних алгебраїчних перетворень у скінченному полі a^0 традиційно дорівнює 1. Ці випадки зазвичай зрозумілі з контексту та не будуть викликати непорозумінь.

Оскільки S-блок є бієктивним тоді і тільки тоді, коли a – генератор мультиплікативної групи поля $\mathbb{F}_{2^n}$, то далі будемо розглядати лише такі елементи $a \in \mathbb{F}^*_{2^n}$, які є генераторами.

Використання додаткових афінних перетворень на вході чи на виході S-блоку дозволяє збільшити кількість доступних для застосування перетворень при збереженні багатьох криптографічних властивостей. Саме в сенсі збереження, зокрема, нелінійності, диференціальних імовірностей та лавинних ефектів ми кажемо про «еквівалентність» S-блоків. Класична EA-еквівалентність розглядає входи та виходи S-блоку як звичайні двійкові вектори; відповідно, афінні перетворення, які використовуються, розглядаються над лінійним векторним простором V_n.

Для експоненційних S-блоків використання EA-еквівалентності не завжди дозволяє зберегти бажані криптографічні властивості, оскільки вхідні значення експоненційного S-блоку фактично є лишками за модулем 2^n, а вихідні значення – елементами скінченного поля $\mathbb{F}_{2^n}$. Тому ми пропонуємо розглянути інший спосіб побудови еквівалентних S-блоків.

Розглянемо афінні перетворення таких двох типів.

1) $A(x) = (u \cdot x + v) \bmod 2^n$, де x, u, v – числа за модулем 2^n, всі операції виконуються за модулем 2^n та $\gcd(u, 2^n) = 1$ (тобто u є непарним числом). За таких обмежень $A(x)$ – невироджене перетворення над $\mathbb{Z}_{2^n}$.
2) $B(x) = c \cdot x \oplus d$, x, c, $d \in \mathbb{F}_{2^n}$, всі операції є операціями з поля та $c \neq 0$. За таких обмежень $B(x)$ – невироджене перетворення над $\mathbb{F}_{2^n}$.

Будемо казати, що S-блоки $s_1(x)$ та $s_2(x)$ є *цілком афінно еквівалентними*, якщо

$$s_2(x) = B(s_1(A(x))).$$

S-блок $s_2(x)$, який є цілком афінно еквівалентним деякому експоненційному S-блоку, будемо називати *розширеним експоненційним S-блоком*. Метою подальшого розгляду є встановлення найпростіших способів будувати розширені експоненційні S-блоки.

Нехай $s(x) = a^x$ – деякий експоненційний S-блок. Застосувавши афінне перетворення лише на вході, одержуємо

$$s(A(x)) = s(u \cdot x + v) = a^{u \cdot x + v}.$$

Позначимо $c = a^v$, $w = a^u$; тоді $s(A(x)) = c \cdot w^x$. Бачимо, що отриманий вираз схожий на результат застосування афінного (навіть лінійного) перетворення на виході S-блоку. Але $s(A(x))$ буде розширеним експоненційним перетворенням лише в тому випадку, коли w – генератор мультиплікативної групи $\mathbb{F}^*_{2^n}$. А w буде генератором тоді і тільки тоді, коли u та $(2^n - 1)$ – взаємнопрості.

Можемо остаточно сформулювати таке твердження: якщо $\gcd(u, 2^n - 1) = 1$, то для довільного експоненційного S-блоку $s(x)$ існує такий експоненційний S-блок $s'(x)$, що $s(A(x)) = B(s'(x))$, причому $B(x) = c \cdot x$. Отже, значна частина афінних перетворень на вході може бути замінена деякими афінними перетвореннями на виході для іншого експоненційного S-блоку. Наприклад, автором було розраховано кількість таких значень $u \in \mathbb{Z}_{256}$, що $\gcd(u, 2^8 - 1) = 1$ та $\gcd(u, 2^8) = 1$; їх виявилось 64, тобто рівно половина від усіх можливих значень. Відповідно, використання таких перетворень одночасно не призводить до збільшення кількості розширених експоненційних S-блоків.

Важливим частковим випадком є використання відображень зсуву $A(x) = x + v$ (тобто афінних перетворень із $u = 1$). У даному випадку маємо

$$s(A(x)) = a^{x+v} = c \cdot a^x = c \cdot s(x) = B(s(x)),$$

тобто зсуви переводять експоненційний S-блок у розширений (на виході) експоненційний S-блок від тієї ж експоненти. Так само, оскільки a є генератором, а c – елементом мультиплікативної групи поля, то $c \cdot s(x) = a^v \cdot a^x = a^{x+v}$.

Підсумовуючи, можемо стверджувати, що для заданого експоненційного S-блоку існує лише два нерівносильні шляхи побудувати цілком афінно еквівалентний S-блок, а саме:

1) використовувати афінні перетворення $A(x) = (u \cdot x + v) \bmod 2^n$ на вході, де $\gcd(u, 2^n - 1) \neq 1$;
2) використовувати афінні перетворення $B(x) = c \cdot x \oplus d$ на виході, де $d \neq 0$.

Дослідженню властивостей таких класів розширених S-блоків планується присвятити подальші дослідження.

Висновки

У даній роботі було введено нове поняття цілком афінної еквівалентності, застосовне до класу експоненційних перетворень над скінченними полями характеристики 2. Показано, що в багатьох випадках різні форми афінних перетворень вхідних та вихідних значень експоненційного S-блоку аналогічні одне одному, та сформульовані типи таких перетворень, які не зводяться одне до іншого. Використання саме таких афінних перетворень дозволить суттєво розширити клас криптографічно стійких S-блоків на основі експоненційних перетворень, однак конкретні криптографічні властивості побудованих таким чином відображень потребують подальших досліджень.

Перелік використаних джерел

1. Agievich Sergey, Afonenko Andrey. Exponential S-boxes. — Cryptology ePrint Archive, Report 2004/024. — 2004. — `https://eprint.iacr.org/2004/024`.
2. Budaghyan Lilya, Carlet Claude. On CCZ-equivalence and its use in secondary constructions of bent functions. — Cryptology ePrint Archive, Report 2009/042. — 2009. — `https://eprint.iacr.org/2009/042`.