УДК 004.056.55:519.2

ЛЕМА ПРО СПАДАННЯ ІМОВІРНОСТЕЙ ДЛЯ УЗАГАЛЬНЕНИХ S-ФУНКЦІЙ

С. В. Яковлєв[1, a]

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

Анотація

В роботі наводяться визначення узагальненої S-функції та її властивості, а також формулюється узагальнення леми Бірюкова-Величкова про спадання імовірностей, необхідної для ефективної автоматичної оцінки стійкості ARX-криптосистем до диференціального криптоаналізу

Ключові слова: симетрична криптографія, диференціальний криптоаналіз, ARX-криптосистеми, S-функції

Вступ

Розвиток та поширення великої кількості малоресурсних систем та пристроїв в побуті (зокрема, в рамках впровадження «інтернету речей») поставив нові задачі захисту конфіденційності інформації: традиційні криптографічні алгоритми, призначені для вирішення цих задач, виявились занадто складними для реалізації на таких пристроях. Тому в останні роки бурхливий розвиток одержала «легка криптографія» (*lightweight cryptography*), метою якої є побудова та аналіз спрощених криптографічних алгоритмів, придатних для реалізації у обчислювально слабких середовищах.

Одним з популярних напрямків легкої криптографії є побудова так званих ARX-криптосистем – алгоритмів, які, в широкому сенсі, використовують лише такі операції, які доступні на рівні інструкцій процесору (зокрема, побітове, модульне додавання та циклічний зсув). Однією з переваг ARX-криптосистем є чітка алгебраїчна структура, яка дозволяє виконувати оцінювання стійкості таких систем до відомих методів криптоаналізу шляхом формалізованих автоматичних обчислень. Методи та платформи для проведення такого автоматичного аналізу постійно розвиваються та оновлюються.

Дана робота присвячена дослідженню властивостей так званих узагальнених S-функцій. Цей математичний апарат дозволить значно розширити перелік алгебраїчних операцій, придатних для побудови та аналізу ARX-криптосистем.

1. Визначення та властивості узагальненої S-функції

Нехай $\mathcal{X}$ – скінченна множина і $\mathcal{D} = \mathcal{X}^n$. Для вектору $x = (x_1, x_2, \ldots, x_m) \in \mathcal{D}$ позначимо через $x[k]$ підвектор $x[k] = (x_1, \ldots, x_k) \in \mathcal{X}^k$.

Відображення $f\colon \mathcal{D}^m \to \mathcal{D}$ є *узагальненою S-функцією* (від англ. *state function*), якщо виконуються такі дві умови:

1) Обчислення вектору $z = f(x^{(1)}, \ldots, x^{(m)})$ представляється у такому вигляді:
$$(z_i, S_{i+1}) = \varphi_i(x_i^{(1)}, \ldots, x_i^{(m)}, S_i),\ i = \overline{1, m},$$
де S_i – допоміжні змінні (стани обчислення), значення яких належать деякій множині $\mathcal{Q}$, початковий стан $S_0 \in \mathcal{Q}$ фіксовано, а відображення $\varphi_i\colon \mathcal{X}^m \times \mathcal{Q} \to \mathcal{X} \times \mathcal{Q}$ – функції обчислення i-тої координати (можливо, різні).
2) Множина значень станів обчислення $\mathcal{Q}$ скінченна та не змінюється при можливій зміні кількості координат n.

Звичайні S-функції, введені Величковим, Мухою та ін. [1], задаються множиною значень $\mathcal{X} = \{0, 1\}$.

Безпосередньо з визначення узагальнених S-функцій випливають такі властивості:

1) Процес обчислення значення узагальненої S-функції подається роботою певного скінченного автомата Мілі із множиною станів $\mathcal{Q}$, множиною сигналів $\mathcal{D}$ та функціями переходу φ_i.
2) Суперпозиція узагальнених S-функцій, визначених на одному домені $\mathcal{X}$, є узагальненою S-функцією.

Нехай $\otimes\colon \mathcal{D} \times \mathcal{D} \to \mathcal{D}$ – бінарна операція, яка задає на множині $\mathcal{D}$ структуру абелевої групи. Тоді з другої властивості випливає таке твердження: якщо відображення $a(x, y) = x \otimes y$ є узагальненою S-функцією, то відображення $b(x, y) = x \otimes y^{-1}$ також є узагальненою S-функцією, де y^{-1} – елемент, обернений до y за операцією $\otimes$. Прикладами операцій, які є узагальненими S-функціями, на множині $\{0, 1\}^n$ можуть бути побітове, модульне та поблокове додавання.

[a] yasv@rl.kiev.ua

Позначимо через $\otimes dp^f$ диференціальну імовірність відображення f за операцією $\otimes$:

$$\otimes dp^f(\alpha_1, \ldots, \alpha_m \to \gamma) = \\ = \Pr_{x^{(1)},\ldots,x^{(m)}}\{f(x_1 \otimes \alpha_1, \ldots, x_m \otimes \alpha_m) = \\ = f(x_1, \ldots, x_m) \otimes \gamma\}.$$

Тоді, якщо відображення f та операція $\otimes$ є узагальненими S-функціями, то диференціальна імовірність $\otimes dp^f$ фактично виступає розподілом деякої узагальненої S-функції, параметризованої значеннями $\alpha_1, \ldots, \alpha_m$ та γ.

2. Лема про спадання імовірностей

Для узагальненої S-функції f позначимо через $f[k]$ *префіксну функцію* – функцію, одержану із функції f зупинкою процесу обчислення на k-тому кроці (після обчислення k-тої координати виходу). Таким чином, якщо $f(x^{(1)}, \ldots, x^{(m)}) = z$, то $f[k](x^{(1)}[k], \ldots, x^{(m)}[k]) = z[k]$.

Має місце таке твердження, яке узагальнює результат, одержаний Бірюковим та Величковим у [2].

Теорема (*лема про спадання імовірностей для узагальнених S-функцій*).

Нехай f – узагальнена S-функція і $z \in \mathcal{D}$. Позначимо $p_0 = 1$ та

$$p_k = \Pr_{x^{(1)},\ldots,x^{(m)}}\{f[k](x^{(1)}[k], \ldots, x^{(m)}[k]) = z[k]\}.$$

Тоді виконуються такі нерівності:

$$p_0 \geqslant p_1 \geqslant \cdots \geqslant p_m.$$

Доведення. Нехай $\mathcal{L}_k$ – множина допустимих входів для фунції $f[k]$, тобто множина наборів векторі

$$\mathcal{L}_k = \{(x^{(1)}, \ldots, x^{(m)}) \in \mathcal{D}^k : \\ f[k](x^{(1)}, \ldots, x^{(m)}) = z[k]\}.$$

Для визначеності встановимо також $\mathcal{L}_0 = \{\varnothing\}$. Тоді

$$p_k = \frac{|\mathcal{L}_k|}{|\mathcal{X}|^{km}}.$$

Із визначення S-функції випливає, що якщо для деякого набору $\left(x^{(1)}, \ldots, x^{(m)}\right) \in \mathcal{D}^m$ виконується рівність

$$f[k+1](x^{(1)}[k+1], \ldots, x^{(m)}[k+1]) = z[k+1],$$

то для нього ж виконується й рівність

$$f[k](x^{(1)}[k], \ldots, x^{(m)}[k]) = z[k],$$

оскільки в цьому випадку процес обчислення $f[k+1]$ просто зупиняється на один крок раніше. Отже, якщо взяти довільний набір векторів з множини $\mathcal{L}_{k+1}$ та прибрати в кожному векторі останню, $(k+1)$-шу координату, то ми повинні одержати певний набір векторів з множини $\mathcal{L}_k$. Таким чином, $|\mathcal{L}_{k+1}| \leqslant |\mathcal{X}|^m \cdot |\mathcal{L}_k|$. Тому

$$p_{k+1} = \frac{|\mathcal{L}_{k+1}|}{|\mathcal{X}|^{(k+1)m}} \leqslant \frac{|\mathcal{X}|^m \cdot |\mathcal{L}_k|}{|\mathcal{X}|^{km+m}} = \frac{|\mathcal{L}_k|}{|\mathcal{X}|^{km}} = p_k,$$

звідки й випливає твердження теореми. □

Наслідок. Лема про спадання імовірностей фактично каже, що розподіли префіксних функцій будь-якої узагальненої S-функції можуть лише домінувати над розподілом значень самої S-функції (з точністю до префікса). Якщо відображення f та бінарна операція $\otimes$ є узагальненими S-функціями, то диференціальні імовірності $\otimes dp^f$ також є розподілами певної узагальненої S-функції та підпадають під твердження теореми. Таким чином, можна оцінювати значення імовірностей $\otimes dp^f$ через значення префіксних імовірностей.

В роботі [2] твердження леми про спадання імовірностей було доведено для звичайних S-функцій та імовірностей диференціалів відносно побітового додавання (xdp) та додавання за модулем 2^n (adp). В даній роботі лема доводиться в загальному вигляді.

Твердження леми та її наслідок мають дуже важливе значення для автоматичного оцінювання стійкості ARX-криптосистем до диференціального криптоаналізу. Дійсно, для заданого відображення f пошук диференціалів із високою імовірністю – дуже важка задача, яка має велику складність перебору. Однак завдяки лемі про спадання імовірностей можна обрати префікси такої довжини, для яких знаходження значень диференціальних імовірностей є простою обчислювальною задачею, і знайти їх всі; після цього префікси, які мають занадто низьку (або навіть нульову) імовірність, треба відкинути, оскільки імовірність будь-якого диференціалу з таким префіксом не може бути більшою. Для префіксів, які залишились, довжина подовжується та переобчислюються імовірності всіх нових префіксних диференціалів, знову відкидаючи занадто малі. Таким своєрідним методом «гілок та границь» можна автоматично знайти всі диференціали, імовірність яких буде не нижчою за встановлене порогове значення.

Висновки

У даній роботі були розглянуті деякі властивості узагальнених S-функцій та доведено в загальній формі лему про спадання імовірностей. Ці результати дозволять значно розширити перелік алгебраїчних операцій, придатних для побудови ARX-криптосистем, та розробити більш точні методи аналізу ARX-криптосистем, зокрема, шляхом автоматичного оцінювання стійкості до диференціального криптоаналізу.

Перелік використаних джерел

1. N. Mouha, V. Velichkov, Chr. De Cannière, B. Preneel. The Differential Analysis of S-Functions // Selected Areas in Cryptography: 17th International Workshop. — SAC'2010, Proceedings. — Springer Berlin Heidelberg, 2010. — pp. 36–56.
2. A. Biryukov, V. Velichkov. Automatic Search for Differential Trails in ARX Ciphers // Topics in Cryptology, the Cryptographer's Track at the RSA Conference 2014. — CT-RSA 2014, Proceedings. — Springer International Publishing, 2010. — pp. 227 – 250.