УДК 512.13:004.021+003.26

КРИПТОГРАФІЧНІ ВЛАСТИВОСТІ РІВНЯНЬ ПЕРШОГО СТЕПЕНЯ ІЗ РІЗНИМИ АЛГЕБРАЇЧНИМИ ОПЕРАЦІЯМИ

Яковлєв Сергій, Кривицька Тетяна, Ломаченко Ігор

НТУУ «КПІ», Фізико-технічний інститут

Анотація

Розглядаються рівняння першого степеня над бітовими векторами від однієї та двох змінних, в яких використовуються різні алгебраїчні операції: побітове, модульне та поблокове додавання. Для таких рівнянь досліджені деякі властивості, які мають застосування у криптографії, зокрема, при диференціальному криптоаналізі певних класів блочних шифрів та при побудові колізій геш-функцій.

Abstract

The point of this research is to obtain cryptographic properties of simple equations with one or two unknowns which uses different algebraic operations: bitwise, modular and blockwise addition over binary vectors. Such properties are widely used in differential cryptanalysis of block ciphers and in search of collision of hash functions.

Вступ

Одним з поширених засобів досягання гарних властивостей криптографічних перетворень, зокрема, високої нелінійності та згладжування статистичних характеристик, є одночасне використання декількох алгебраїчних операцій, таких як побітове та модульне додавання. Як приклади можна привести національний стандарт шифрування ДСТУ ГОСТ 28147:2009, сімейство геш-функцій MD (MD4, MD5), сучасні ARX-алгоритми. При аналізі стійкості таких симетричних шифрів та геш-функцій часто постають задачі дослідження властивостей лінійних рівнянь, що використовують різні операції. В даній роботі наводяться відомості щодо деяких типів таких рівнянь.

Тут і надалі через V_n позначено простір *n*-бітних векторів. На просторі V_n ми розглядаємо операції $\oplus$ (побітове додавання) та + (додавання за модулем 2^n, при цьому бітові вектори розглядаються як двійковий запис відповідних чисел). Також, якщо $n = u \cdot m$, то простір V_n можна розглядати як простір $(V_u)^m$, на якому визначено операцію по блокового додавання $[+]$: для $x, y \in V_n$ маємо $x[+]y = (x_1 + y_1, ..., x_m + y_m)$, де $x_i, y_i \in V_u$ – відповідні координати векторів, а додавання виконується за модулем 2^u.

Дослідження рівнянь виду $x + \alpha = x \oplus \beta$ та $x[+]\alpha = x \oplus \beta$

Рівняння виду $x + \alpha = x \oplus \beta$ для фіксованих векторів α та β виникають при проведенні диференціального криптоаналізу симетричних шифрів, при побудові колізій на геш-функції та при побудові атак збоїв на криптопримітиви, в структурі яких присутні як побітове, так і модульне додавання. Втім, в опублікованих джерелах не було представлено систематичного аналізу таких рівнянь. Нижче ми наводимо деякі результати, які мають криптографічне значення.

1) Рівняння $x + \alpha = x \oplus \beta$ має розв'язки тоді та тільки тоді, коли виконується рівність:

$$(\neg(\beta << 1)) \wedge (\alpha \oplus \beta \oplus (\alpha << 1)) = 0, \qquad (1)$$

де $\neg$ та $\wedge$ – операції логічного НІ та логічного АБО, які застосовуються до кожного біта окремо, а через $<<1$ позначено нециклічний зсув вектору на один біт в сторону старших

розрядів (із відкиданням старшого). Зазначимо, що умова розв'язуваності (1) легко перевіряється на практиці.

2) Якщо рівняння $x+\alpha = x \oplus \beta$ має розв'язки (тобто виконується умова (1)), то їх кількість дорівнює $2^{wt(\neg(\beta<<1))}$, де через $wt(.)$ позначено вагу Хемінга (кількість одиничних біт вектору). Таким чином, ліва частина рівняння не впливає на кількість розв'язків, а впливає лише на розв'язуваність системи взагалі.

3) Запропоновано простий комбінаторний алгоритм побудови множини всіх можливих розв'язків. Цей алгоритм лінійний відносно довжини векторів *n* та може бути розпаралелений; фактично він обчислює кожен окремий біт розв'язку виходячи з таких умов:

якщо біт $\beta_i = 0$, то біт x_i може приймати довільне значення;

якщо біт $\beta_i = 1$, то біт $x_i = \alpha_{i+1} \oplus \beta_{i+1}$.

(Для старшого біту *x* потрібна додаткова корекція.)

4) Запропоновано прості комбінаторні алгоритми побудови за заданим фіксованим вектором α множини всіх векторів β та за заданим фіксованим вектором β множини всіх векторів α, для яких рівняння $x+\alpha = x \oplus \beta$ є розв'язуваним. Ці алгоритми також лінійні відносно *n* і піддаються паралелізації.

Наведемо алгоритм побудови зазначеної множини векторів β за заданим вектором α. Всі вектори будуються ітеративно та побітово, у порядку зростання номерів бітів.

біт $\beta_0 = \alpha_0$;

якщо біт $\beta_{i-1} = 0$, то біт β_i може приймати довільне значення;

якщо біт $\beta_{i-1} = 1$, то біт $\beta_i = \alpha_i \oplus \alpha_{i-1}$.

Аналогічний алгоритм для побудови множини векторів α за заданим вектором β буде виглядати таким чином:

біт $\alpha_0 = \beta_0$;

якщо біт $\beta_{i-1} = 1$, то біт α_i може приймати довільне значення;

якщо біт $\beta_{i-1} = 0$, то біт $\alpha_i = \beta_i \oplus \alpha_{i-1}$.

При диференціальному криптоаналізі блочних шифрів, що використовують S-блоки, часто більш ефективним буде розглядання операції $[+]$ замість + для побудови різниць. Для рівнянь виду $x[+]\alpha = x \oplus \beta$ природно переносяться всі наведені вище результати, оскільки воно фактично розпадається на *m* незалежних рівнянь виду $x_i + \alpha_i = x_i \oplus \beta_i$ для векторів довжини *u*. Більш цікаві рівняння виду $x+\alpha = x[+]\beta$, яким буде присвячено подальші дослідження.

Диференціальні властивості різних операцій додавання

Ліпмаа та Моріаі дослідили рівняння виду $(x \oplus \alpha)+(y \oplus \beta) = (x+y) \oplus \gamma$, які відповідають властивостям функції $f(x,y) = x+y$ при проведенні диференціального криптоаналізу відносно операції ⊕. Зокрема, ними були виведені умова розв'язуваності таких систем, відповідні розподіли імовірностей

$$xdp^{+}(\alpha,\beta \to \gamma) = \frac{1}{2^{2n}} \left| \{x, y \in V_n : (x \oplus \alpha)+(y \oplus \beta) = (x+y) \oplus \gamma \} \right|,$$

та ефективні алгоритми їх обчислення для конкретних значень векторів. Далі Ліпмаа та ін. і Валлен розглянули інший варіант рівнянь, $(x+\alpha)\oplus(y+\beta)=(x\oplus y)+\gamma$, які відповідають властивостям функції $g(x,y)=x\oplus y$ при проведенні диференціального криптоаналізу відносно операції $+$. Цей варіант виявився значно складнішим для аналізу, однак дослідниками була розроблена методологія обчислення відповідних імовірностей

$$adp^{\oplus}(\alpha,\beta\to\gamma)=\frac{1}{2^{2n}}\left|\left\{x,y\in V_n:(x+\alpha)\oplus(y+\beta)=(x\oplus y)+\gamma\right\}\right|.$$

Узагальнення результатів Ліпмаа та його співавторів на відповідні рівняння із операцією $[+]$ відбуваються природнім чином в силу блокової структури самої операції. Так, маємо:

$$xdp^{[+]}(\alpha,\beta\to\gamma)=\prod_{i=1}^{m}xdp^{+}(\alpha_i,\beta_i\to\gamma_i).$$

При розгляданні диференціальних властивостей функції $g(x,y)=x\oplus y$ відносно операції $[+]$ та відповідних імовірностей

$$bdp^{\oplus}(\alpha,\beta\to\gamma)=\frac{1}{2^{2n}}\left|\left\{x,y\in V_n:(x[+]\alpha)\oplus(y[+]\beta)=(x\oplus y)[+]\gamma\right\}\right|,$$

маємо таке співвідношення:

$$bdp^{\oplus}(\alpha,\beta\to\gamma)=\prod_{i=1}^{m}adp^{\oplus}(\alpha_i,\beta_i\to\gamma_i).$$

Більший інтерес становлять рівняння виду $(x+\alpha)[+](y+\beta)=(x[+]y)+\gamma$ та $(x[+]\alpha)+(y[+]\beta)=(x+y)[+]\gamma$ і відповідні їм імовірності $adp^{[+]}(\alpha,\beta\to\gamma)$ та $bdp^{+}(\alpha,\beta\to\gamma)$, яким планується присвятити подальші дослідження.

Список використаних джерел:

1. Кривицька Тетяна Сергіївна. Диференціальні властивості криптографічних перетворень, що використовують модульне та побітове додавання : магістерська дисертація / Кривицька Тетяна Сергіївна. – К.: НТУУ «КПІ», 2014. – 92 с. – Бібліогр. : с. 91-92.
2. Lipmaa Helger. Efficient Algorithms for Computing Differential Properties of Addition [електронний ресурс] / H. Lipmaa, S. Moriai. – Режим доступу: http://eprint.iacr.org/2001/001
3. Lipmaa Helger. On the Additive Differential Probability of Exclusive-Or [електронний ресурс] / H. Lipmaa, J. Wallén, Ph. Dumas. – Режим доступу: http://pdf.aminer.org/000/217/216/on_the_additive_differential_probability_of_exclusive_or.pdf
4. Johan Wallén. On the Differential and Linear Properties of Addition : Ph.D. theses [електронний ресурс] / J. Wallén. – Режим доступу: http://www.tcs.hut.fi/Publications/bibdb/HUT-TCS-A84.pdf