Перевірка Модельних Припущень у Криптоаналізі Arx-Шифрів

Олександр Деркач
кафедра математичних методів захисту інформації
Фізико-технічний інститут
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»
Київ, Україна
alex7derkach@gmail.com

Verification of Model Assumptions in Cryptanalysis of Arx-Ciphers

Oleksandr Derkach
Department of Mathematical Methods of Information Security
Institute of Physics and Technology
National Technical University of Ukraine "Igor Sikorsy Kyiv Polytechnic Institute"
Kyiv, Ukraine
alex7derkach@gmail.com

***Анотація*—На прикладі шифру ARX-ГОСТ експериментально перевірені модельні припущення двох найпоширеніших методів аналізу ARX-криптосистем – диференціального та обертального криптоаналізу.**

***Abstract*—We present experimental verification of model assumptions for two the most popular methods of ARX-ciphers cryptanalysis – differential and rotational cryptanalysis, applied to ARX-GOST cipher.**

Ключові слова—ARX-криптосистеми, диференціальний криптоаналіз, обертальний криптоаналіз, шифр ГОСТ

Keywords—ARX-cryptosystems, differential cryptanalysis, rotational cryptanalysis, GOST cipher

I. Вступ

ARX-криптосистеми (від англ. Add-Rotation-Xor) – окремий клас криптопримітивів, побудованих лише із застосуванням операцій модульного та побітового додавання, а також циклічного зсуву бітових векторів. Такі операції підтримуються усіма сучасними обчислювальними архітектурами на рівні базових, що дозволяє будувати надшвидкі криптопримітиви. Протягом останніх років було запропоновано багато криптографічних алгоритмів на основі ARX, зокрема, потокових шифрів (Salsa, ChaCha), блокових шифрів (Simon, Speck), геш-функцій (BLAKE, Skein) тощо. Для потокових шифрів швидкість роботи має важливе значення, тому дослідження ARX-примітивів в цьому напрямку є актуальною задачею.

У той же час методи аналізу стійкості ARX-криптосистем ґрунтуються здебільшого на експериментальних обчисленнях та модельних припущеннях, справжність яких іноді виглядає сумнівною. У даній роботі на прикладі конструкції ARX-ГОСТ буде розглянуто адекватність таких припущень для двох найпоширеніших в наш час методів аналізу ARX-криптосистем – диференціального та обертального криптоаналізу. Відштовхуючись від одержаних даних, будуть визначені параметри конструкції ARX-ГОСТ, за яких вона досягає максимальної стійкості до диференціального криптоаналізу.

II. Теоретичні відомості

Нехай V_n – множина всіх n-бітових векторів, на якій визначено три операції: операція $<<<$ циклічного зсуву вектора на один біт, операція $\oplus$ побітового додавання та операція $+$ додавання за модулем 2^n; при цьому вважається, що бітові вектори природним чином ототожнені із лишками кільця $\mathbf{Z}_2^n$: кожне число ототожнюється із вектором власного представлення у двійковій системі числення. *ARX-криптосистемою* будемо називати криптопримітив, побудований лише з використанням введених трьох операцій.

Стійкість ARX-криптосистем ґрунтується на тому, що операція додавання за модулем є складним нелінійним перетворенням над полем $\mathbf{F}_2$. Будемо називати *диференціалом* трійку векторів $(\alpha, \beta \to \gamma)$, які задовольняють рівнянню

$$(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma,$$

а відповідну імовірність такої події (*xor differential probability*) позначимо через

$$xdp^{+}(\alpha, \beta \to \gamma) = Pr_{x,y}\{(x \oplus \alpha) + (y \oplus \beta) = (x + y) \oplus \gamma\}.$$

Аналітичні умови для перевірки існування диференціалів такого типу із ненульовими імовірностями, обчислення значення імовірностей, оцінки кількості та розподіли нетривіальних диференціалів, а також алгоритми пошуку диференціалів та їх окремих векторів із максимально можливими значеннями імовірностей наведені у роботі [1].

Багато існуючих досліджень стійкості ARX-криптосистем ґрунтується на експериментальному обчисленні максимумів імовірності диференціалів. При цьому зазвичай висувається *гіпотеза про марковську поведінку імовірностей*: імовірності проходження диференціалів через кожну операцію + вважаються незалежними, що дозволяє обчислювати імовірності диференціалів складних ARX-конструкцій шляхом звичайного множення імовірностей на окремих їх вузлах. Однак справедливість даної гіпотези не підтверджена, а для інших конструкцій симетричної криптографії (наприклад, SP-мереж із модульним додаванням у ключовому суматорі) ця гіпотеза не виконується. Тому в даному розділі буде проведена експериментальна перевірка гіпотези про марковість окремих ARX-примітивів.

Іншим методом криптоаналізу ARX-конструкцій є *обертальний криптоаналіз* (*rotational cryptanalysis*) [2]. Цей метод споріднений до диференціального криптоаналізу, але замість диференціалів в якості досліджуваної статистики розглядаються так звані *пари обертання* – пари векторів виду (x, x'), де $x' = x >>> r$ для певного фіксованого значення r. Пари обертання однозначно проходять через операцію $\oplus$ та циклічні зсуви. Імовірність проходження пар обертання через операцію + була встановлена у [3] (див. також [4]):

$$p(r) = Pr_{x,y}\{(x + y)' = x' + y'\} = \frac{1}{4}\left(1 + \frac{1}{2^r} + \frac{1}{2^{n-r}} + \frac{1}{2^n}\right).$$

При обертальному криптоаналізі ARX-криптосистем також часто висувалось припущення про маркову поведінку імовірностей проходження пар обертання через операції додавання; в цьому випадку імовірність проходження пари обертання через всю систему обчислювалась як $(p(r))^q$, де q – кількість операцій додавання за модулем у системі. Втім, вже самими розробниками даного методу встановлено, що за наявності в системі декількох операцій додавання підряд така оцінка є неадекватно заниженою [5]. Далі буде показано, що таке модельне припущення не буде виконуватись навіть якщо всі операції додавання у ARX-криптосистемі розмежовані побітовими додаваннями та циклічними зсувами.

Основною конструкцією, яка досліджується в даній роботі, є блоковий шифр ARX-ГОСТ, одержаний із блокового шифру ДСТУ ГОСТ 28147:2009 [6] (далі – просто ГОСТ) шляхом усунення S-блоків із раундової функції. Важливість такої конструкції зумовлена легкістю її реалізації на існуючих апаратних та апаратно-програмних рішеннях (оскільки вона, власне, є модифікованим шифром ГОСТ). Формалізуємо шифр ARX-ГОСТ у вигляді такого сімейства відображень.

Раундове перетворення F є параметризованим за двома параметрами n, r ключезалежним перетворенням виду:

$$F: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n \times \{0,1\}^n,$$

$$F_k(x, y) = (y, x \oplus ((y + k) <<< r)).$$

Тут n – довжина вхідного напівблоку, r – величина циклічного зсуву. Раундові ключі k також розглядаються як n-бітові вектори.

Шифр ARX-ГОСТ є ітеративним блоковим шифром, який складається із послідовного застосування раундових перетворень F із незалежними рівноімовірними раундовими ключами. Шифр ARX-ГОСТ, який складається з m раундів, будемо позначати через F^m; раундові ключі $k_1, \ldots, k_m$ для зручності запису будемо опускати.

III. Перевірка модельних припущень диференціального та обертального криптоаналізу для шифру ARX-ГОСТ

Блокові шифри, які використовують у ключовому суматорі додавання за модулем замість побітового додавання, зазвичай втрачають властивість марковості: імовірності раундових диференціалів перестають бути незалежними, оскільки вони будуть напряму залежати від значення точки входу. Продемонструємо це на такому простому прикладі.

Нехай S – 8-бітовий S-блок шифру AES (можна використати довільний криптографічний S-блок) і $g_k(x) = S[x + k]$. Двохраундовий шифр E визначимо як

$$E_{k_1,k_2}(x) = g_{k_2}(g_{k_1}(x)),$$

де раундові ключі k_1 та k_2 є незалежними та рівноімовірними.

Визначимо імовірності диференціалів шифру E двома способами: шляхом безпосереднього обчислення за визначенням:

$$P_1\{\alpha \to \beta\} = \frac{1}{\left(2^8\right)^3}\sum_x \sum_{k_1,k_2}\left[E_{k_1,k_2}(x \oplus \alpha) = E_{k_1,k_2}(x) \oplus \beta\right],$$

(тут квадратними дужками позначено індикаторну функцію – дужки Айверсона), а також через імовірності диференціальних характеристик, припускаючи, що такий шифр є марковським:

$$d^g(\alpha,\beta)=\frac{1}{2^{16}}\sum_x\sum_k\left[g_k(x\oplus\alpha)=g_k(x)\oplus\beta\right],$$

$$P_2\{\alpha\to\beta\}=\sum_\gamma d^g(\alpha,\gamma)d^g(\gamma,\beta).$$

Обчислення по всіх диференціалах (α, β) показали, що:

1) для 65005-ти диференціалів з 65536-ти можливих (тобто у 99.19%) значення імовірностей P_1 та P_2 відрізняється, причому у 32510-ти диференціалах (49.61% від загальної кількості розбіжних) істинна імовірність більша за модельну, а у 32495-ти (50.39%) – менша;

2) загальна середня квадратична відстань між істинними розподілами імовірностей диференціалів та модельними розподілами складає ≈ 0.027, тобто доволі суттєву величину з точки зору статистичної розрізнюваності.

Таким чином, експериментально встановлено, що при використанні різних алгебраїчних операцій блокові шифри втрачають властивість марковості. Тобто при аналізі блокових шифрів довільної структури необхідно завжди доводити чи спростовувати гіпотезу про марковість перетворень.

Далі експериментальним шляхом було перевірено, чи виконується гіпотеза про марковість для шифру ARX-ГОСТ. Через брак обчислювальних ресурсів була перевірена зменшена версія шифру із розміром напівблоку $n = 4$ та величиною внутрішнього циклічного зсуву $r = 1$.

Неважко показати, що імовірності раундових диференціалів шифру ARX-ГОСТ зводяться до імовірностей xdp^+ таким чином:

$$d^F(\alpha,\beta)=[\alpha_2=\beta_1]\,xdp^+(\alpha_2,\,0\to(\alpha_1\oplus\beta_2)>>>r),$$

де вхідна та вихідна різниці розбиваються на дві n-бітові частини: $\alpha=(\alpha_1,\alpha_2)$, $\beta=(\beta_1,\beta_2)$.

Відповідно, для m-раундового шифру ARX-ГОСТ необхідно порівняти значення істинних імовірностей диференціалів

$$P_1\{\alpha\to\beta\}=$$

$$=\frac{1}{2^{2n}}\frac{1}{\left(2^n\right)^m}\sum_{(x,y)}\sum_{k_1,\ldots,k_m}\left[F^m(x\oplus\alpha_1,y\oplus\alpha_2)=F^m(x,y)\oplus\beta\right],$$

із розрахунковою модельною імовірністю

$$P_2\{\alpha\to\beta\}=\sum_{\gamma_1,\ldots,\gamma_{m-1}}d^g(\alpha,\gamma_1)d^g(\gamma_1,\gamma_2)\ldots d^g(\gamma_{m-1},\beta).$$

Обчислення імовірностей всіх диференціалів для $m = 2$, 3 та 4 раундів шифрування показало, що для шифру ARX-ГОСТ гіпотеза про марковську поведінку імовірностей диференціалів повністю виконується: істинні значення імовірностей всіх диференціалів співпали із модельними. Таким чином, для оцінювання стійкості шифру ARX-ГОСТ до диференціального криптоаналізу можна використовувати припущення про марковість. Це дуже важливий результат з огляду на суттєвішу спрощенність аналітичного дослідження марковських шифрів у порівнянні із немарковськими. Втім, необхідно пам'ятати, що результати експериментальних обчислень в даному випадку потребують аналітичного підтвердження перед застосуванням під час оцінювання стійкості конкретних шифрів.

На наступному етапі дослідження була перевірена гіпотеза про марковість імовірностей пар обертання у шифрі ARX-ГОСТ. Для цього для різних значень зсуву s між векторами x та $x' = x >>> s$ порівнювалась істинна імовірність

$$P_1=Pr_{x,y,k_1,\ldots,k_m}\left\{F^m(x',y')=F^m(x,y)'\right\}$$

(тут обертання як на вході, так і на виході виконується над кожним напівблоком окремо, що виправдане структурою шифру) із модельною імовірністю

$$P_2=\left(p(s)\right)^m.$$

Результати обчислень наведені у таблиці 1.

ТАБЛИЦЯ I. РІЗНИЦІ ІМОВІРНОСТЕЙ ПАР ОБЕРТАННЯ

m	**Зсув на 1**		
	Модельне	***Істинне***	***Різниця***
2	0.178	0.178	0
3	0.075085	0.073261	0.001823
m	**Зсув на 2**		
	Модельне	***Істинне***	***Різниця***
2	0.153	0.153	0
3	0.059605	0.053963	0.005642
m	**Зсув на 3**		
	Модельне	***Істинне***	***Різниця***
2	0.178	0.178	0
3	0.075085	0.073261	0.001823

З табл. 1 видно, що припущення про марковість для імовірностей пар обертання у шифрі ARX-ГОСТ перестає виконуватись вже починаючи з третього раунду. Для шифру ARX-ГОСТ бачимо, що теоретична (модельна) імовірність має більше значення, аніж істинне, тому загальна оцінка стійкості до обертального криптоаналізу не повинна порушитись; однак невідомо, чи буде така залежність справджуватись для більшої кількості раундів та для інших ARX-примітивів.

IV. Пошук параметрів шифру ARX-ГОСТ, які максимізують стійкість до диференціального криптоаналізу

Наступною задачею даного дослідження є визначення параметрів шифру ARX-ГОСТ, за яких даний шифр є найбільш захищеним від диференціального криптоаналізу. Знову розглядалась зменшена восьмибітова версія шифру (n = 4), для якої визначалась максимальна імовірність диференціалів в залежності від величини внутрішнього зсуву r.

Оскільки в попередньому розділі було експериментально встановлено, що для шифру ARX-ГОСТ виконується припущення про марковість, для обчислення імовірностей диференціалів була обрана більш проста формула $P_2\{\alpha \rightarrow \beta\}$, яка використовує імовірності диференціальних характеристик. Стійкість шифру до диференціального криптоаналізу визначалась за двома параметрами:

максимальним значенням імовірності диференціалу (повинна бути мінімально можливою для посилення стійкості шифру);

кількістю диференціалів, які мають максимальну імовірність (повинно бути якомога менше для ускладнення пошуку таких диференціалів).

Результати експериментальних обчислень наведені у таблиці 2.

ТАБЛИЦЯ II. Максимуми імовірностей диференціалів та їх кількість (у дужках) в залежності від зсуву та кількості раундів

Кількість раундів	***r = 1***	***r = 2***	***r = 3***
2	0.5 (32)	0.5 (32)	0.5 (32)
3	0.5 (8)	0.5 (6)	0.5 (10)
4	0.5 (2)	0.5 (4)	0.5 (4)
5	0.25 (5)	0.5 (2)	0.25 (7)
6	0.125 (2)	0.25 (6)	0.125 (6)

З табл. 2 випливає, що найкращі показники стійкості шифру ARX-ГОСТ за двома параметрами досягаються при значенні внутрішнього зсуву r = 1. Таким чином, можна припустити, що для загальної конструкції шифру ARX-ГОСТ максимальна стійкість до диференціального криптоаналізу також буде досягатись при невеликих значеннях внутрішнього зсуву, зокрема, можливо, також на один біт.

V. Висновки

У даній роботі був проведений аналіз модельних припущень у диференціальному та обертальному криптоаналізі ARX-криптосистем на прикладі зменшеного восьмибітового шифру ARX-ГОСТ. Експериментально показано на прикладі S-блоку шифру AES, що не для будь-яких конструкцій виконується гіпотеза марковості імовірностей диференціалів. У той же час показано, що для конструкції ARX-ГОСТ це припущення виконується, що дозволяє значно спростити аналіз стійкості такого шифру. Але аналогічне припущення про незалежність імовірностей пар обертання для шифру ARX-ГОСТ порушується.

Ґрунтуючись на одержаних результатах, було знайдено величину внутрішнього зсуву для шифру ARX-ГОСТ, за якої такий шифр сягає максимальної стійкості до диференціального криптоаналізу. Виявилось, що внутрішній зсув повинен бути невеликий: для зменшеної версії шифру найкращі результати показав шифр із внутрішнім зсувом у один біт. Такий зсув зменшить максимум імовірності диференціала і зменшить загальну кількість таких диференціалів.

Результати даної статті можуть використовуватись для побудови нових стійких криптопримітивів, зокрема, потокових шифрів та блокових шифрів у режимах вироблення гами, на основі ARX-конструкцій, а також для аналізу існуючих алгоритмів легкої криптографії.

Подальші дослідження даної теми передбачають перевірку модельних припущень для збільшених версій шифру ARX-ГОСТ – 16 та 32 бітних і аналітичне обгрунтування побудованих моделей. Також для покращення параметрів шифру варто врахувати оцінки стійкості до обертального криптоаналізу.

Література References

[1] H. Lipmaa, S. Moriai, “Efficient algorithms for computing differential properties of addition” in *Lecture Notes in Computer Science*, Springer, 2001, vol. 2355, pp. 1-17.

[2] D. Khovratovich and I. Nikolic, “Rotational cryptanalysis of ARX” in *Fast Software Encryption*: 17th International Workshop (FSE 2010), Seoul, Korea, February 7-10 2010. Lecture Notes in Computer Science, vol. 6147, Springer, 2010, pp. 333–346.

[3] Th. A. Berson, “Differential cryptanalysis mod n with applications to MD5” in *Advances in Cryptology*: CRYPTO ’92. Lecture Notes in Computer Science, vol. 740, Springer-Verlag, 1993, pp. 71–80.

[4] M. Daum, “Cryptanalysis of hash functions of the MD4-Family,” Ph.D. thesis , Ruhr-Universität Bochum, May 2005.

[5] D. Khovratovich, I. Nikolic, J. Pieprzyk, Prz. Sokolowski and R. Steinfeld, “Rotational cryptanalysis of ARX revisited” [Online]. Available: http://eprint.iacr.org/2015/095

[6] Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89), ДСТУ ГОСТ 28147:2009.