ДОСЛІДЖЕННЯ КРИТЕРІЇВ ЯКОСТІ ТА РОЗРОБКА АЛГОРИТМУ ГЕНЕРАЦІЇ ДОВГОСТРОКОВИХ КЛЮЧОВИХ ЕЛЕМЕНТІВ ШИФРАТОРА ГОСТ 28147-89

Сергій Яковлєв

Національний технічний університет України "Київський політехнічний інститут",
Фізико-технічний інститут, Київ, проспект Перемоги, 37.
E-mail: yasv@rl.kiev.ua

Abstract

A problem of creation of long-term keys for GOST 28147-89 is considered. Balance set of S-box criteria was formulated; S-box generation algorithm was proposed.

Алгоритм шифрування даних, описаний у стандарті ГОСТ 28147-89, окрім звичайного ключа шифрування, включає в себе так званий довгостроковий ключовий елемент – блоки заміни, що складаються з восьми вузлів заміни (нелінійних перетворень спеціального вигляду). Однак в стандарті не наведено жодних вимог та правил вибору до блоку заміни; зазначається лише, що блоки заміни повинні поставлятися установленим порядком.

В рамках даного дослідження ми висунемо вимоги, яким повинні відповідати криптографічно стійкі вузли заміни, а також сформулюємо критерії відбору вузлів з можливим уточненням вимог та наведемо алгоритм генерації довгострокових ключових елементів для практичного використання у існуючих реалізаціях алгоритма ГОСТ 28147-89.

Були сформульовані такі загальні вимоги до вузлів заміни:

1) Кожен вузол заміни повинен бути перестановкою.
2) Координатні функції вузлів заміни повинні:
   а) бути збалансованими;
   б) бути нелінійними;
   в) мати низьку кореляцію між вхідними та вихідними значеннями;
   г) мати відчутний лавинний ефект.
3) Використання знайдених вузлів заміни не повинно послаблювати стійкість алгоритму до відомих криптоаналітичних атак (лінійного криптоаналізу, диференціального криптоаналізу, атак на реалізації).
4) Кількість ДКЕ, вузли заміни яких задовольняють висунутим вимогам, повинна бути такою, щоб додатково унеможливити їх повний перебір за прийнятний час.

За допомогою попередніх обчислень встановлено, що існує 2328 координатних функцій, що відповідають наведеним вимогам (всі ці функції були знайдені та збережені для подальшого використання). З них можна побудувати 15 926 114 304 різних перестановочних вузлів заміни, з яких, в свою чергу, можна створити щонайменше $4{,}2\cdot10^{80}$ різних ДКЕ.

Для одержаних вузлів були сформульовані вимоги щодо їх характеристик, які показують вплив на стійкість загального перетворення до різних видів криптоаналізу (лінійного, діференціального, а також атак за живленням та часом): лінійне відхилення, діференціальне відхилення, рівень прозорості. Оцінена кількість вузлів, що відповідає цим вимогам: 2,01·109 таких, що протидіють лінійному та диференціальному аналізу, з них 1,4·109 таких, що додатково протидіють атакам на реалізацію. З такої кількості вузлів можна одержати щонайменше 3·1068 різних ДКЕ.

Також розглянуті додаткові критерії на вузли заміни, що показують на можливі уразливості перетворення.

Користуючись одержаною сукупністю критеріїв, були оцінені характеристики відомих ДКЕ, що рекомендовані різними стандартами та нормативними документами (зокрема, "Інструкцією про порядок постачання і використання ключів до засобів криптографічного захисту інформації", наказ ДержСпецЗв'язку №114 від 12.06.2007).

Сформульовано алгоритм генерації вузлів заміни та довгострокових ключових елементів:

1) Обрати чотири довільних функції, що задовольняють висунутим вимогам (всі ці функції знайдені попередньо).
2) Побудувати на основі вибраних функцій вузол заміни.
3) Якщо побудований вузол не є перестановкою, повернутися до пункту 1.
4) Якщо є вимога щодо відсутності нерухомих точок – перевірити наявність нерухомих точок у вузлі. Якщо нерухомі точки є, повернутися до пункту 1.
5) Обчислити значення лінійного відхилення вузла. Якщо це значення не дорівнює 4, повернутися до пункту 1.

6) Обчислити значення діференціального відхилення вузла. Якщо це значення більше 6, повернутися до пункту 1.

7) Якщо висунута така вимога, перевірити значення рівня прозорості. Якщо значення є неприйнятним – перейти до пункту 1.

Побудований вузол заміни вдовольняє висунутим вимогам та може використовуватися. Для генерації довгострокового ключового елементу необхідно згенерувати вісім вузлів. Програмна реалізація вимагає 7-8 мілісекунд на генерацію одного ДКЕ (не враховуючи передобчислення).

Наведений алгоритм може бути запропонований як кандидат на ліцензування в ДержСпецЗв'язку (якщо будуть розглядатися інші алгоритми генерації ДКЕ) та застосовуватися в системах шифрування даних та як складова функції гешування ГОСТ 34.311-95.

Дане дослідження може розглядатися як робота в рамках періодичної перевірки криптостійкості алгоритму ГОСТ 28147-89.

Література:

[1] ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов, 1989. – 26 с.
[2] Мухачёв В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полиграф-Консалтинг», 2005 – 214 с.
[3] Холоша А.А. Об одном подходе к аналізу качества блока подстановки битовых векторов. // Збірник наукових праць ІПМЕ НАН України. Вип. 2. Львів: Світ, 1998. – С.59-74
[4] B. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems // Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991
[5] C. Carlet. On highly nonlinear S-boxes and their inability to thwart DPA attacks // Cryptology ePrint Archive (http://eprint.iacr.org/2005/387)
[6] M. Matsui. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology – EUROCRYPT '93 (Lecture Notes in Computer Science no. 765), Springer-Verlag, pp. 386-397, 1994
[7] Amr Mohammed Youssef. Analysis and Design of Block Ciphers (doctoral thesis). – Ontario, Queen's Univeresity, 1997
[8] RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.
[9] ДержСпецЗв'язку, наказ №114 від 12.06.2007, "Інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації".
[10] Горбенко И.Д., Лисицкая И.В. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. Всеукр. межвед. науч.-техн. сб. 1997. Вып. 103. С. 121-130.
[11] Горбенко И.Д., Лисицкая И.В., Коряк А.С. Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа. // Радиоэлектроника и информатика. 1998. №1 (02). С. 39-43
[12] Лисицкая И.В. Противоречивые подстановки в алгоритме ГОСТ 28147-89//. Информационные системы: Сб. научн. тр.- Харьков: НАНУ, ПАНУ, ХВУ, 1995. 9 с.
[13] Логачёв О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М. Издательство МЦНМО, 2004. – 472 с.