Перевірка «випадковості» генерації S-блоків алгоритму шифрування ДСТУ 7624:2014

М.П. Оксьоненко
кафедра математичних методів захисту інформації,
Фізико-технічний інститут,
Національний технічний університет Україні
«Київський політехнічний інститут»,
Київ, Україна
maksoks94@gmail.com

С.В. Яковлєв
кафедра математичних методів захисту інформації,
Фізико-технічний інститут,
Національний технічний університет Україні
«Київський політехнічний інститут»,
Київ, Україна
yasv@rl.kiev.ua

Testing the “random” generation of S-boxes of encryption algorithm DSTU 7624:2014

M. Oksonenko
Department of Mathematical Methods of Information Security,
Institute of Physics and Technology,
National Technical University of Ukraine
“Kyiv Polytechnic Institute”
Kyiv, Ukraine
maksoks94@gmail.com

S. Yakovlev
Department of Mathematical Methods of Information Security,
Institute of Physics and Technology,
National Technical University of Ukraine
“Kyiv Polytechnic Institute”
Kyiv, Ukraine
yasv@rl.kiev.ua

***Анотація* — Перевірено криптографічні властивості S-блоків шифру ДСТУ 7624:2014 «Калина» та його попередньої версії 2007-го року. Показано, що S-блоки останньої версії були знайдені не шляхом випадкового пошуку.**

***Abstract* — We examine some cryptographic properties of S-boxes of DSTU 7624:2014 (“Kalyna”) cipher and its previous 2007-year version. We show that S-boxes of last version of this cipher cannot be randomly generated.**

Ключові слова — S-блок; таблиця імовірностей диференціалів; таблиця імовірностей лінійних апроксимацій

Keywords — S-box; difference distribution table; linear approximations table

I. Вступ

Швидкий розвиток інформаційних технологій зумовив розвиток і впровадження криптографічних алгоритмів і протоколів в різні сфери нашого життя. Питання захисту конфіденційності даних постає майже в усіх системах електронної обробки даних. Блокові шифри є поширеним криптопримітивом для забезпечення конфіденційності. Складові сучасних блокових шифрів обираються через призму відомих методів криптоаналізу для забезпечення самого високого рівня надійності. Однак методи криптоаналізу постійно вдосконалюються, тому необхідно постійно проводити ретроспективну оцінку криптографічної стійкості наявних алгоритмів.

У 2015 році в Україні був прийнятий новий національний стандарт блокового шифрування ДСТУ 7624:2004 («Калина») [1]. Розробники стверджують, що одні з головних структурних одиниць даного шифру, таблиці нелінійної заміни (S-блоки), були одержані шляхом випадкового пошуку. В даній роботі за допомогою статистичного аналізу це твердження буде перевірено.

II. Необхідні терміни та позначення

S-блок – функція, що приймає на вхід n біт і перетворю їх за визначеним правилом, видаючи на виході m біт. n та m не обов’язково рівні між собою. Якщо $m = n$, то мова йде про бієктивний S-блок. В шифрах, які ми розглядаємо, використовуються саме бієктивні перетворення.

Нехай $f : \{0,1\}^n \to \{0,1\}^n$ – деяке відображення.

Таблиця імовірностей диференціалів (Difference Distribution Table, DDT) відображення f – матриця $\|d_{ij}\|$ розмірності $2^n \times 2^n$, де кожний елемент d_{ij} знаходиться за формулою:

$$d_{ij} = \left|\{x \in \{0,1\}^n : f(x \oplus i) \oplus f(x) = j\}\right|.$$

Таблиця імовірностей лінійних апроксимацій (Linear Approximation Table, LAT) відображення f – матриця $\left\|c_{ij}\right\|$ розмірності $2^n \times 2^n$, де кожний елемент c_{ij} знаходиться за формулою:

$$c_{ij} = \left|\{x \in \{0,1\}^n : x \cdot i = f(x) \cdot j\}\right| - 2^{n-1} = \tfrac{1}{2}\sum_x (-1)^{x \cdot i \oplus f(x) \cdot j}.$$

Імовірності диференціалів та лінійних апроксимацій визначають стійкість криптоперетворень до диференціального та лінійного криптоаналізу.

III. Перевірка S-блоків на «випадковість»

Розробники шифру «Калина» декларували, що S-блоки даного алгоритму одержані шляхом випадкового пошуку: генерувалась випадкова підстановка, яка перевірялась на ряд умов на криптографічні параметри; підстановки, які не задовольняли умовам, відкидались. Табличне представлення замість аналітичного визначення (як то зроблено, скажімо, в шифрі AES) було обрано спеціально для захисту від алгебраїчних атак.

Існують теоретичні оцінки для певних статистичних параметрів випадкових S-блоків – зокрема, визначено теоретичну імовірність, що для випадкового S-блоку максимальне значення λ таблиці DDT (LAT) буде зустрічатись не більше ніж N разів [4]. За допомогою цих параметрів можна встановити, скільки необхідно перебрати випадкових S-блоків, щоб знайти S-блок із заданими параметрами.[3]

Для DDT 8-бітного S-блоку відповідна імовірність оцінюється за такою формулою:

$$\Pr(\lambda, N) = \sum_{t=0}^{N} C_{255^2}^{t} D(\lambda)^t \left(\sum_{d=0}^{\frac{\lambda}{2}-1} D(2d)\right)^{255^2 - t},$$

де $D(2d) = \dfrac{e^{-\frac{1}{2}}}{2^d\, d!}$ – імовірність розподілу Пуассона із параметром ½. Аналогічна формула для LAT має вид

$$\Pr(\lambda, N) = \sum_{t=0}^{N} C_{255^2}^{t} (L(\lambda) + L(-\lambda))^t \left(\sum_{d=-\frac{\lambda}{2}+1}^{\frac{\lambda}{2}-1} L(2d)\right)^{255^2 - t},$$

де $L(2d) = \dfrac{\left(C_{128}^{64+d}\right)^2}{C_{256}^{128}}$ – імовірність гіпергеометричного розподілу.

Нами було розглянуто вісім S-блоків $S_0,...,S_7$ з шифру «Калина» 2007 р. [2] та чотири S-блоки $\pi_0,...,\pi_3$ з шифру «Калина» 2014 р [1]. Для кожного з них побудовано таблицю імовірності диференціалів і таблицю імовірністю лінійних апроксимацій та обчислено значення параметрів λ, N та $\Pr(\lambda, N)$. Результати обчислень наведено у таблиці І.Значення імовірностей $\Pr(\lambda, N)$ для DDT та LAT S-блоків шифрів «Калина»

Таблиця І. Значення імовірностей $\Pr(\lambda, N)$ для DDT та LAT S-блоків шифрів «Калина»

S-блок	***DDT***			***LAT***		
	λ	N	$\Pr(\lambda, N)$	λ	N	$\Pr(\lambda, N)$
π_0	8	15	$\approx 2^{-90}$	24	44	$\approx 2^{-200}$
π_1	8	9	$\approx 2^{-100}$	24	28	$\approx 2^{-240}$
π_2	8	7	$\approx 2^{-120}$	24	42	$\approx 2^{-200}$
π_3	8	9	$\approx 2^{-100}$	24	40	$\approx 2^{-200}$
S_0	8	90	$\approx 2^{-18}$	32	2	$\approx 2^{-6}$
S_1	8	80	$\approx 2^{-20}$	30	6	$\approx 2^{-6}$
S_2	8	96	$\approx 2^{-18}$	32	2	$\approx 2^{-6}$
S_3	8	96	$\approx 2^{-18}$	32	4	$\approx 2^{-5}$
S_4	8	91	$\approx 2^{-18}$	32	8	$\approx 2^{-5}$
S_5	8	93	$\approx 2^{-18}$	32	5	$\approx 2^{-5}$
S_6	8	101	$\approx 2^{-18}$	32	3	$\approx 2^{-6}$
S_7	8	105	$\approx 2^{-18}$	32	3	$\approx 2^{-5}$

З наведених даних бачимо, що S-блоки $S_0,...,S_7$ першої версії шифру «Калина» цілком могли бути знайдені шляхом випадкового пошуку: складність такого пошуку в середньому становить $2^{18} \div 2^{20}$ перебору. Однак випадковий пошук S-блоків із параметрами підстановок $\pi_0,...,\pi_3$ вимагатиме $2^{100} \div 2^{200}$ спроб. Тому можна стверджувати, що S-блоки $\pi_0,...,\pi_3$ щонайменше були певним аналітичним чином покращені для підсилення стійкості до диференціального та лінійного криптоаналізу.

IV. Висновки

Було показано, що генерація S-блоків алгоритму шифрування ДСТУ 7624:2014 «Калина» шляхом випадкового пошуку вимагає занадто великої кількості ресурсів (на відміну від генерації S-блоків попередньої версії шифру «Калина» 2007 року). Відповідно, можна стверджувати, що для генерування цих S-блоків використовувались певні аналітичні алгоритми, оцінка впливу яких на загальну криптографічну стійкість шифру наразі є недослідженою.

Література References

[1] R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, O. Dyrda, V. Dolgov, A. Pushkaryov, R. Mordvinov, D. Kaidalov. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. – 2015. – http://eprint.iacr.org/2015/650

[2] Горбенко І.Д. Перспективний блоковий шифр "Калина" – основні положення та специфікація / І.Д. Горбенко, О.С. Тоцький, С.В. Казьміна та ін. // Прикладна радіоелектроніка. – 2007. – Т.6, №2. – С.195-208

[3] A. Biryukov, L. Perrin and A. Udovenko. Reverse-Engineering the S-Box of Streebog, Kuznyechik and STRIBOBr1 (Full Version). – 2016. – http://eprint.iacr.org/2016/071

[4] J. Daemen, V. Rijmen. Probability distributions of correlation and diffrentials in block ciphers // Journal of Mathematical Cryptology. – №1(3). – 2007