ПОДХОДЫ К ФОРМИРОВАНИЮ ПОДСТАНОВОК С ОПТИМАЛЬНЫМИ ПОКАЗАТЕЛЯМИ

Казимиров А.В.
Научный руководитель – к.т.н., доц. Олейников Р.В.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. БИТ, тел. (057) 702-14-25),
E-mail: bit@kture.kharkov.ua; факс (057) 702-14-25

В работах Ниберг [1] ещё в 1991 году приводятся методы построения подстановок с предельными дифференциальными и линейными показателями. Однако в последнее время всё больше стали показывать свою эффективность атаки, основанные на характеристиках булевых функций и алгебраическая атака [2]. Это связано с тем, что идеи, изложенные в Rijndael, стали применяться во многих криптосистемах.

Помимо метода, предложенного Ниберг, есть множество других способов по генерации S-блоков. Например, алгоритмы случайных шагов, основанных на конечном автомате и др [3]. Однако все эти методы не учитывают особенности алгебраических атак.

Существуют методы генерации S-боков на основе булевых функций. В работе [4] предложен метод по генерации подстановок с хорошими (с точки зрения характеристик булевых функций) показателями. Однако остаётся открытым вопрос об уровне значимости большинства известных показателей булевых функций. Если нелинейность и автокорреляция связаны соответственно с линейными и дифференциальными показателями S-блоков, то не совсем ясны мотивы введения критериев: строгого лавинного, корреляционной иммунности, распространения. Эти критерии применяются при анализе поточных шифров, но необходима оценка их влияния на стойкость блочных симметричных шифров.

Кроме того, стоит отметить последнюю работу [5], посвящённую переосмыслению подходов для оценки значения полного дифференциала. В данной работе показывается, что значение полного дифференциала не зависит от подстановок, применяемых в шифре. Однако, отмечается, что S-блок влияет на динамические показатели шифра, т.е. на то, как быстро шифр приходит к теоретическому среднему максимуму дифференциальной таблицы. Это означает, что подстановки с хорошими показателями гораздо эффективней, чем сгенерированные случайным образом.

В таблице 1 приводятся результаты расчёта количества уравнений, описывающих подстановки, показатели булевых функций, максимума дифференциальной и линейной таблицы. Представленные значения рассчитывались для подстановок, применяемых в шифрах AES, Camellia, Лабиринт, Калина.

Таблица 1 – характеристики подстановок

	AES	Cam.	Lab.	K0	K1	K2	K3	K7
Сбаланси-рованность БФ	ДА	ДА	ДА	ДА	ДА	ДА	ДА	ДА
NL	112	112	112	96	98	96	96	96
AC	32	32	32	88	88	88	104	96
SQA	133120	133120	133120	244480	252928	259456	291712	251392
SAC	0	0	0	0	0	0	0	0
PC	0	0	0	0	0	0	0	0
CI	0	0	0	0	0	0	0	0
Resilient	0	0	0	0	0	0	0	0
Наименьшая степень БФ	7	7	7	7	7	6	7	7
Количество уравнений	39	39	39	441	441	441	441	441
Степень уравнений	2	2	2	3	3	3	3	3
Инверсии	ДА	НЕТ	ДА	НЕТ	НЕТ	НЕТ	НЕТ	ДА
Циклы	ДА	НЕТ	ДА	ДА	ДА	НЕТ	ДА	ДА
Возрастания	ДА	НЕТ	ДА	НЕТ	НЕТ	ДА	ДА	ДА
MDT	4	4	4	8	8	8	8	8
MLT	16	16	16	32	30	32	32	32
Биектив-ность	ДА	ДА	ДА	ДА	ДА	ДА	ДА	ДА

1. Nyberg, K. Perfect nonlinear S-boxes. [Text] // K. Nyberg. // Eurocrypt. - 1991. Vol. 547 - pp. 378-386.
2. Courtis N. T. Cryptanalysis of Block Cipher with Overdefined System of Equations [Electronic resource] / N. T. Courtois, J. Pieprzyk. // Mode of access : WWW.URL: http://goo.gl/lgIMZ – Last access: 2011. – Title from the screen.
3. Kazmi S. Random Walk Algorithm Based Design Technique for S-Box [Text] // S. Kazmi, N. Ikram. International Journal of Cryptology Research. 2009. pp. 65-72.
4. Seberry J. Systematic Generation of Cryptographically Robust S-boxes [Electronic resource] / J. Seberry, Xian-Mo Zhang, Y. Zheng // Mode of access: WWW.URL: http://goo.gl/7sLyt – Last access: 2011. – Title from the screen.
5. Долгов В.И. Вариации на тему шифра Rijndael [Текст] / В.И. Долгов, И.В. Лисицкая, А.В. Казимиров // Прикладная радиоэлектроника. Том 9 №3 – Харьков, - 2010.