О критерии распространения криптографических классов булевых функций

Исаев Глеб Андреевич

Аспирант

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: ichimaru-gin512@yandex.ru

Научный руководитель *— Логачев Олег Алексеевич*

Булевы функции активно применяются в компьютерных системах в целях улучшения комбинаторных, криптографических и прочих свойств этих систем. Для соответствия булевой функции многим из указанных выше свойств важно, чтобы булева функция обладала оптимальным набором криптографических характеристик, среди которых существенную роль играет так называемый критерий распространения.

Понятие критерия распространения булевых функций представляет собой множество векторов, для которых соответствующие им производные булевой функции являются уравновешенными функциями. Оно характеризует статистические свойства семейства производных булевой функции, играющих важную роль в анализе и синтезе криптосистем. Впервые понятие критерия распространения было введено Бартом Пренеелем и соавторами в работе [5] в целях характеризации стойкости применяемых в шифрах булевых функций к линейным и дифференциальным методам криптоанализа, успешное проведение которых дает много информации о секретном ключе (подробно об этих методах см. [1] и [3]). Кроме того, для некоторых классов булевых функций критерий распространения определяет их экстремальные свойства. Например, максимальное значение количества векторов, удовлетворяющих критерию распространения, имеет место лишь при чётном числе переменных и для экстремального класса булевых функций, называемых бент-функциями, а минимальное значение достигается только у аффинных функций.

В работе получены точные значения и оценки количества векторов, удовлетворяющих критерию распространения булевых функций из известных криптографических классов, таких как платовидные функции, функции из класса Майорана–МакФарланда, квадратичные функции, алгебраически вырожденные функции и мультиаффинные функции. Также получены необходимые и достаточные условия принадлежности векторов множеству критерия распростра-

нения монотонно неубывающих функций, наименьший носитель которых состоит из одного или двух векторов, и соответствующих им монотонно невозрастающих функций.

Литература

1. Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
2. Ященко В. В. О критерии распространения для булевых функций и о бент-функциях // Проблемы передачи информации. 1997. Т. 1, № 33. С. 75–86.
3. Carlet C. Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge, 2020.
4. Carlet C., Joyner D., Stănică P., Tang D. Cryptographic properties of monotone Boolean functions // Journal of Mathematical Cryptology, De Gruyter, vol. 10, № 1, 2016, P. 1–14.
5. Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J. Propagation characteristics of Boolean functions // Advances in Cryptology — EUROCRYPT'90, Lecture Notes in Computer Science, Springer–Verlag, Berlin, Heidelberg, New-York, vol. 473, 1991, P. 161–173.