Секция «Математика»

Характеризация булевых функций с мощностью множества критерия распространения, равной $2^n - 2$

Исаев Глеб Андреевич
Аспирант
Московский государственный университет имени М.В.Ломоносова, Факультет вычислительной математики и кибернетики, Кафедра информационной безопасности, Москва, Россия
E-mail: ichimaru-gin512@yandex.ru

Изучение критерия распространения и его свойств является одним из важнейших направлений исследований в области криптографических приложений булевых функций. Булева функция удовлетворяет критерию распространения по направлению (определяемому вектором из соответствующего n-мерного булева пространства), если производная данной функции по этому направлению является уравновешенной функцией. Совокупность всех таких направлений (векторов) для булевой функции называют множеством её критерия распространения.

Необходимо отметить, что для некоторых классов булевых функций критерий распространения связан с их экстремальными свойствами. Например, для максимально-нелинейных булевых функций (или бент-функций) множество критерия распространения содержит в себе все ненулевые векторы из соответствующего n-мерного булева пространства, в то время как для аффинных функций оно не содержит в себе ни одного вектора.

В работе рассмотрен вопрос существования булевых функций, близких с точки зрения критерия распространения к бент-функциям, то есть таких функций, у которых все векторы, кроме нулевого и одного некоторого ненулевого вектора, удовлетворяют критерию распространения. Показано, что множество булевых функций с таким свойством существует только при нечётном числе переменных. Кроме того, изучен вопрос принадлежности множества булевых функций с этим свойством к каким-либо криптографическим классам и, в том числе, к классам корреляционно-иммунных и устойчивых функций, а также выявлено взаимно однозначное соотношение между этими функциями и бент-функциями.

Источники и 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) Исаев Г. А. Критерии распространения различных классов булевых функций и их свойства // International Journal of Open Information Technologies. 2021. Т. 9, № 5. С. 18–24.
3) Carlet C. Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge, 2020.
4) Potapov V. N., Taranenko A. A., Tarannikov Yu. V. Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces // arXiv: 2108.00232 [math.CO], 2021, P. 1–10
5) Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J. Propagation characteristics of Boolean functions // EUROCRYPT'90, Lecture Notes in Computer Science, Springer–Verlag, vol. 473, 1990, P. 161–173.