

Аналогичным [3] образом нами получено точное значение MEDP двух раундов шифра Khazad [2] среди дифференциалов веса 9 :

$$\text{MEDP}_{\text{Khazad}}^9 = 2^{-45} + 2^{-60}. \quad (1)$$

Получена оценка

$$\text{MEDP}_{\text{Khazad}}^{10} \leq 2^{-44.31\dots}. \quad (2)$$

на дифференциал веса $\Theta + 1$.

Следствием (1) и (2) является следующая оценка MEDP двухраундового шифра Khazad

$$\text{MEDP}_{\text{Khazad}} \leq 2^{-44.31\dots},$$

что улучшает тривиальную оценку [6] на дифференциал двухраундового LSX-шифра: $\text{MEDP}_{\text{Khazad}} \leq 2^{-43.19\dots}$.

Благодаря известной двойственности [5] между дифференциальным и линейным криптоанализом, рассматриваемый способ вычисления оценок на вероятность дифференциала может использоваться и для вычисления оценок на суммарные линейные характеристики шифра.

Полученные оценки будут в дальнейшем применяться при оценке стойкости большего числа раундов LSX-шифра к дифференциальному криптоанализу.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 34.12-2015. Криптографическая защита информации. Блочные шифры. М.: Стандартиформ, 2015.
2. *Barreto P., Rijmen V.* The Khazad legacy-level block cipher. In: First Open NESSIE Workshop (Leuven, 13–14 November 2000). Leuven: Leuven Kath. Univ., p. 15.
3. *Kiryukhin V.* Exact maximum expected differential and linear probability for 2-round Kuznyechik. In: 7th Workshop on Current Trends in Cryptology (CTCrypt 2018). — Матем. вопросы криптографии, 2019, т. 10, в. 2 (в печати).
4. *Hardy G. H., Littlewood J. E., Pólya G.* Inequalities. 2nd ed. Cambridge: Cambridge Univ. Press, 1952. (Ser. Cambridge Mathematical Library.)
5. *Biham E.* On Matsui's linear cryptanalysis. In: Advances in Cryptology. — EUROCRYPT'94. Heidelberg etc.: Springer, 1995, p. 341–355. (Ser. Lect. Notes Comput. Sci. V. 950.)
6. *Park S., Sung S. H., Lee S., Lim J.* Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES. In: Fast Software Encryption — FSE 2003. Heidelberg etc.: Springer, 2003, p. 247–260. (Ser. Lect. Notes Comput. Sci. V. 2887.)