МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 29–38

УДК 519.719.2

Lower bounds for the practical secrecy of a key

I. M. Arbekov

JSC "InfoTeCS", Moscow

Получено 17.III.2016

Abstract. We obtain lower bounds for the *practical secrecy* of a key. *Practical secrecy* is defined as the average amount of keys tested before the *encryption* key is determined. To find the *encryption* key we use truncated key search algorithms having some *success* probabilities. The lower bounds of the *practical secrecy* are expressed in terms of limiting values of success probabilities and of total variation distance between the key probability distribution and the uniform distribution.

Key words: practical secrecy of a key, truncated key search, symmetric cryptography

Нижние оценки для практической секретности ключа

И. М. Арбеков

ОАО «ИнфоТеКС», Москва

Аннотация. В работе получены нижние оценки *практической секретности* ключа. *Практическая секретность* определяется как среднее число опробованных ключей до определения ключа *шифрования*. Для определения ключа *шифрования* мы используем усеченные алгоритма поиска ключа, имеющие некоторые вероятности *успеха*. Нижняя оценка *практической секретности* выражается через предельное значение вероятности *успеха* и расстояние по вариации между распределением ключей и равномерным распределением.

Ключевые слова: практическая секретность ключа, усеченный поиск ключа, симметричная криптография

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 29–38 (Russian)

References

[1] Arbekov I. M., “Criteria of key security”, *Mathematical Aspects of Cryptography*, **7**:1 (2016), 41–58 (in Russian).

[2] Portmann C., Renner R., “Cryptographic security of quantum key distribution”, arXiv: 1409.3525v1 [quant-ph] 11 Sep 2014.