A function $f \in B_n$ is called k-dimensional [1], $k \in \overline{0,n-1}$, if set (3) generates a subspace (in V_n) whose dimension is no greater than k or, equivalently, if set (2) contains at least $n-k$ linearly independent vectors.

Denote by $B_n(k)$ the set of all k-dimensional functions of n variables, $k \in \overline{0,n-1}$. It is well known that, for values of k that are moderate in comparison with the value of n, functions close to k-dimensional ones possess cryptographic weaknesses, which allows one to make some attacks on keystream generators that are constructed from such functions [4–6]. In this connection, an important problem is to construct an efficient algorithm for testing a Boolean function for k-dimensionality.

Note that, to check the condition $f \in B_n(k)$ for a function $f \in B_n$ specified by a vector of values (a truth table), a natural deterministic algorithm can be used whose complexity amounts to $O(n^2 2^n)$ binary operations. This algorithm consists of computing all values of numbers (1) with the help of the fast Walsh–Hadamard transform (see, for instance, [2], p. 217), constructing set (3), and finding a basis of vector space (4) by the Gaussian elimination method. A function f is k-dimensional if and only if the obtained basis contains at least $n-k$ vectors. As is obvious, this algorithm is practically inapplicable if the value of n is sufficiently large (for example, $n \geq 64$) and the function f is obtained with the help of an oracle (i.e., an algorithm computing values of $f(x)$ from arbitrary input arguments $x \in V_n$).

In [1], a probabilistic algorithm or a test for k-dimensionality is proposed that, for any function $f \in B_n$ obtained with the help of an oracle and numbers $k \in \overline{0,n-1}$ and $\varepsilon \in (0,1)$ verifies the main hypothesis H_0 that $f \in B_n(k)$ against the following alternative H_1: $d(f, B_n(k)) \geq 2^n \varepsilon$. This algorithm consists of generating independent random equiprobable vectors $h_1, \ldots, h_l \in V_n$ and testing the equalities

$$f(h_j \oplus Z_{ij}) = f(Z_{ij}), \quad i \in \overline{1,m}, \tag{5}$$

for each $j \in \overline{1,l}$, where $h_1, \ldots, h_l$ are random equiprobable vectors from V_n that are mutually independent and independent of Z_{ij}. Denote by ν_l the number of values $j \in \overline{1,l}$ for which equalities (5) hold. Then the hypothesis H_0 is accepted if $\frac{\nu_l}{l} \geq 0.9 \cdot 2^{-k}$ and is rejected otherwise. In [1], it is proposed to choose $l = 2^k C$ and $m = 2^k k \varepsilon^{-1} C'$, where $C, C' = \text{const}$, which leads to the estimate of the algorithm complexity equal to $O(n 2^{2k} k \varepsilon^{-1})$ binary operations.

For estimating the first kind error probability (i.e., the probability that the test will not "recognize" that a k-dimensional function is k-dimensional), the following form of the Chernov inequality is used in [1]:

$$\mathbf{P}\left(\frac{\nu_l}{l} < 0.9 \cdot 2^{-k} \mid H_0\right) \leq \mathbf{P}\left(\frac{\nu_l}{l} - \mathbf{E}\frac{\nu_l}{l} < -0.1 \cdot 2^{-k} \mid H_0\right) \leq \exp\left\{-0.02 \cdot \frac{C}{2^k}\right\}. \tag{6}$$

Note that the expression in the right side of inequality (6) depends on k and does not converge to zero if k is an (arbitrarily slowly) increasing function of n, for example, $k = \lceil \log n \rceil$, $n \to \infty$.

Below, a more efficient test for k-dimensionality is proposed whose complexity equals $O(n 2^k k^2 \varepsilon^{-1})$ binary operations. The upper bound of the first kind error probability for the test is independent of k, and the upper bound for the second kind error probability is actually the same as that for the test from [1]. In addition, it is also shown that, after some natural change in the alternative H_1, a one-sided test for k-dimensionality (with the first kind error probability equal to zero) can be constructed whose complexity equals $O(n(2^k + k\varepsilon^{-2}) \log (2^k + k\varepsilon^{-2}))$ binary operations.

Let us formulate the main results. The key idea underlying the proposed test is as follows: vectors $h_1, \ldots, h_l$ are not randomly chosen but are formed with the help of an auxiliary procedure in such a way that the set of these vectors belong to the set I_f with high probability if f is a k-dimensional function. To this end, we consider the restriction of the function f to a randomly chosen subspace of the vector space V_n. Note that the idea to use such restrictions in testing properties of Boolean functions apparently goes back to L. Levin's results [7] and underlies a number of probabilistic algorithms for testing degrees of polynomials in several variables over the 2-element field [8, 9]. In the present paper, this idea is implemented as follows.

Denote by $F_{m \times n}$ the set of all $m \times n$ matrices over the field F. For each matrix $X \in F_{t \times n}$, where $k < t < n$, we put $f_X(u) = f(uX)$, $u \in V_t$.