Определения псевдослучайного генератора и псевдослучайной функции

В последующем определении A_k - полиномиальный вероятностный алгоритм ($A_k \in PPT$, $A_k : \{0,1\}^k \to \{0,1\}$), p - полином, $x \leftarrow U_k$ строка $x \in \{0,1\}^k$ является случайной величиной с равномерным распределением, заданным на множестве всех битовых строк длины k.

Определение Семейство функций $\{G_k\}_{k\in\mathbb{N}}$, $G_k : \{0,1\}^{b_k} \to \{0,1\}^k$ называется псевдослучайным генератором, если

$$\forall \{A_k\}_{k\in\mathbb{N}} \, \forall p \, \exists k_0 : \ \forall k \geq k_0$$

$$|P\{A_k(x) = 1\} - P\{A_k(y) = 1\}| \leq \frac{1}{p(k)}$$

$$x \leftarrow G_k(U_{b_k}), y \leftarrow U_k$$

Сложность вычисления G_k в книжных определениях не упоминается. Будем считать, что G_k вычисляется за $O(poly(k))$ детерминированным алгоритмом.

В определении псевдослучайной функции $\{A_k^{F^k(\cdot)}\}_{k\in\mathbb{N}}$ - семейство алгоритмов, входом для каждой из которых являются функция $F^k(x)$: $\{0,1\}^{b_k} \to \{0,1\}^{c_k}$, a_k, b_k - возрастающие натуральные последовательности, а результатом их работы является один бит $\{0,1\}$. В ходе работы каждому алгоритму из $\{A_k^{F^k(\cdot)}\}_{k\in\mathbb{N}}$ предоставлен оракульный доступ к вычислению функции F^k,R^k - случайно выбираемая функция такого же, что и F^k, вида, распределение ее равномерное и задано на множестве всех таких функций, p-полином, $s \in \{0,1\}^k$ - случайная битовая строка с равномерным распределением, заданным на множестве всех битовых строк длины k.

Определение Семейство функций $\{F_s^k(x)\}_{k\in\mathbb{N}}$ называется псевдослучайной функцией, если

$$F_s^k(x) : \{0,1\}^k \times \{0,1\}^{b_k} \to \{0,1\}^{c_k}, \ k \in \mathbb{N}$$

$$\forall \{A_k^{F^k(\cdot)}\}_{k\in\mathbb{N}} \, \forall p \, \exists k_0 : \ \forall k \geq k_0$$

$$|P\{A_k^{F_s^k(\cdot)} = 1\} - P\{A_k^{R^k(\cdot)} = 1\}| \leq \frac{1}{p(k)}$$

Вероятность вычисляется в уменьшаемом - по всем случайным шагам алгоритма A_k и выбору битовой строки s длины k, а в вычитаемом - по всем случайным шагам A_k и по выбору функции R^k.