

Notation 0.1 The expression $X(n) \leq \text{negl}(n)$ means that, for polynomial p , for large n , $X(n) \leq \frac{1}{p(n)}$.

Def 0.2 A function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is *one-way* if (1) $f \in P$, and (2) for every prob poly algorithm A ,

$$\Pr_{x \in \{0,1\}^n} [A(f(x), 1^n) \in f^{-1}(f(x))] \leq \text{negl}(n).$$

If in addition f is length preserving and, for all n , f restricted to $\{0, 1\}^n$ is 1-1 then f is a *one-way permutation* (Note: Definition can be modified to work on functions which have domain $D \in P$.)

Example 0.3 One possible example the function $f(p, q) = pq$ where p, q are n -bit primes. Another example is $f_{p,g}(x) = g^x \pmod{p}$ where p is prime and g generates Z_p .

Def 0.4 Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$. A function $hc : \{0, 1\}^* \rightarrow \{0, 1\}$ is a *hard core predicate* for f if (1) $hc \in P$, and (2) for every prob poly time A

$$\Pr_{x \in \{0,1\}^n} [A(f(x)) = hc(x)] \leq \frac{1}{2} + \text{negl}(n).$$

Def 0.5 Let $L(n) > n$. Let $G : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be such that G restricted to $\{0, 1\}^n$ has image $\{0, 1\}^{L(n)}$. G is a *psuedorandom generator* if for all prob poly A

$$|\Pr_{r \in \{0,1\}^{L(n)}} [A(r) = 1] - \Pr_{s \in \{0,1\}^n} [A(G(s)) = 1]| \leq \text{negl}(n).$$

Notation 0.6 Let $F : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$. Then F_k is the function $F_k(x) = F(k, x)$. F is *length preserving* if, for every $k \in \{0, 1\}^n$ then F_k is length preserving.

Notation 0.7 Let $FUNC_n$ be the set of all functions from $\{0, 1\}^n$ to $\{0, 1\}^n$.

Def 0.8 Let $F : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ be length preserving and in P . F is a *psuedorandom function* if for all oracle Prob Poly machines A

$$|\Pr_{k \in \{0,1\}^n} [A^{F_k}(1^n) = 1] - \Pr_{f \in FUNC_n} [A^f(1^n) = 1]| \leq \text{negl}(n).$$