3.1 Computational Security

Assumptions:

* Security is only guaranteed against efficient adversaries that run in some feasible amount of time.
* Adversaries can potentially succeed (i.e., security can potentially fail) with some very small probability.

3.1.1 The Concrete Approach

* A scheme is  secure if any adversary running for time at most *t* succeeds in breaking the scheme with probability at most .

3.1.2 The Asymptotic Approach

* We view the running tie of any adversary, as well as its success probability, as functions of the security parameter (rather than as concrete numbers). Then:
  + We equate “efficient adversaries” with randomized (or probabilistic) algorithms running in time polynomial in n. (We let PPT stand for “probabilistic polynomial-time.”) this means there exists some polynomial p such that the adversary runs for time at most  when the security parameter is n. We also require for reasons of real-world efficiency that honest parties run in polynomial time, though we stress that the adversary may be much more powerful (and run much longer than) the honest parties.
  + We equate the notion of “small probability of success” with success probabilities smaller than any inverse polynomial in *n* (see Definition 3.4). Such probabilities are called negligible.
* A definition of asymptotic security then takes the following general form:
  + *A scheme is* **secure** *if any PPT adversary succeeds in breaking the scheme with at most negligible probability.*