Perfect Secrecy

Perfect Secrecy w/ Equal Distribution:



Theorem:

Perfect Secrecy 

Relaxed Definition:

1. Allow adversary a small probability E of breaking encryption scheme

()

A Statistical Security (Stat Test)



Equivalent probability of adversary’s distinguishability advantage: 

Still Implies 

1. Allow adversary a limited computational time.

* Polynomial Time Tests
* Can make assumptions based on Communication Model
* Quantum Cryptography
* Beacon of random mathematical modes (high rates)
  + - Example: Solar Flares, Unpredictable Data
* Noisy Communication Channel

Section 2

“Fun w/ security definitions”

Shannon secrecy:

(Gen, Enc, Dec) is Shannon-secret if for all distributions over the message space M, for all m, and for all c in C, seeing a cipher text doesn’t tell adversary any knowledge about the message.