Some Notes

Public Key Cryptosystem(PKC)

- E: encryption function, public,
- D: decryption function, private, it's difficult to compute D from E.
- Examples: RSA
- easy to compute but hard to invert
- drawbacks:
  - inverting may be easy for plaintexts of some special forms
  - easy to compute at least partial info of the plaintext

Semantic Secure

- M is the collection of all possible messages, p_m is the prob. that m is sent, $f : M \to V$.
- Game1: randomly pick $m \in M$, ask the adversary to guess the value of $f(m)$
- Game2: let adversary choose a function f, randomly pick $m \in M$, compute an encryption of m and give it to the adversary, ask him to guess $f(m)$.
- semantically secure: cannot win Game2 with **high** prob. than Game1、
- 与"瞎猜"相比，不能以更显著的概率从密文猜出出明文

Goldwasser-Micali Encryption Scheme

Key generator $\mathcal{K}$

- select primes p,q
- n:=pq
- select a **pseudosquare** y
- public key (n,y), private key (p,q)

Encyption $\mathcal{E}$

- input: m = m1m2...m_l
- for i = 1..l do
  - select x randomly
  - if m_i = 0 then c_i := x^2 else c_i := yx^2
- return (c_1,c_2,...,c_l)

Decryption $\mathcal{D}$

- for i = 1..l do
  - compute e_i = $(\frac{c_i}{p})$
  - if e_i = 1 then m_i := 0 else m_i :=1
- return (m_1, m_2, ..., m_l)

Semantically security of QRP

- semantic secure $\Leftrightarrow$ indistinguishable

References:

- Shafl Goldwasser et al., Probabilistic Encryption
- Georg J. Funchsbauer et al., **An intro. to probabilistic Encryption**
- https://en.wikipedia.org/wiki/Semantic_security
- https://en.wikipedia.org/wiki/Ciphertext_indistinguishability