CSE509: (Intro to) Systems Security

Fall 2012

Radu Sion

Semantic Security

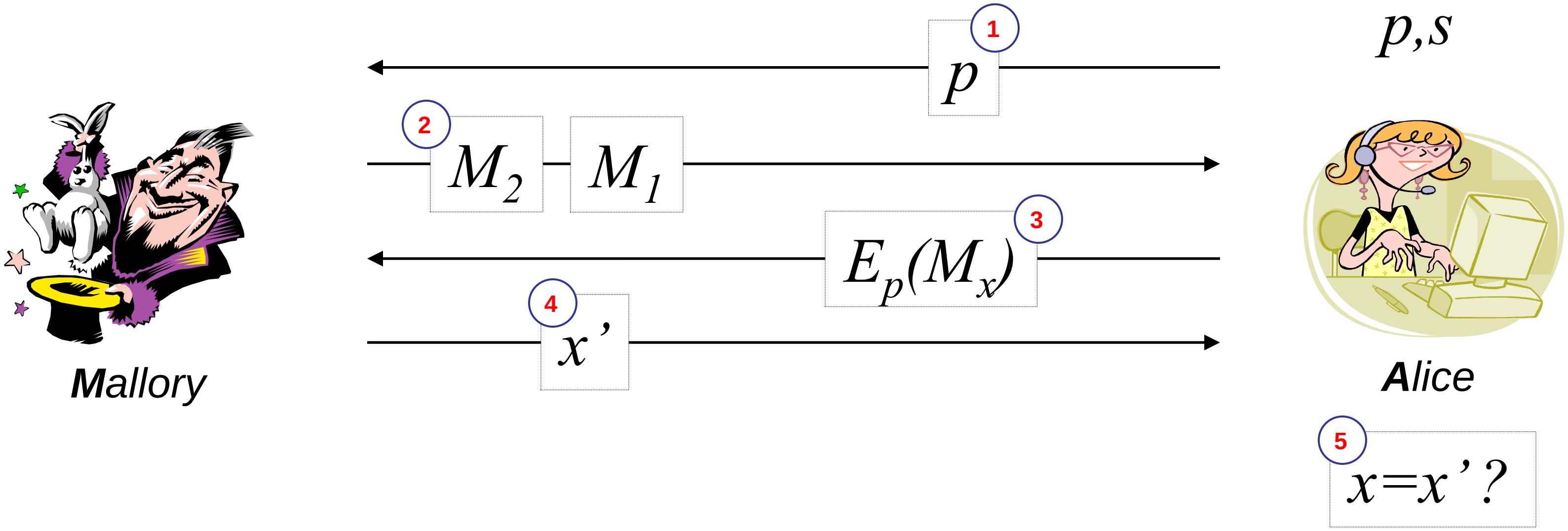
© 2005-12

Perfect Security ?

- Security: plaintext recovery, key recovery
- Perfect: One Time Pad
  - Impractical !
- What else ?
  - Computationally restricted adversary
    - Come up with “close to perfect” security.

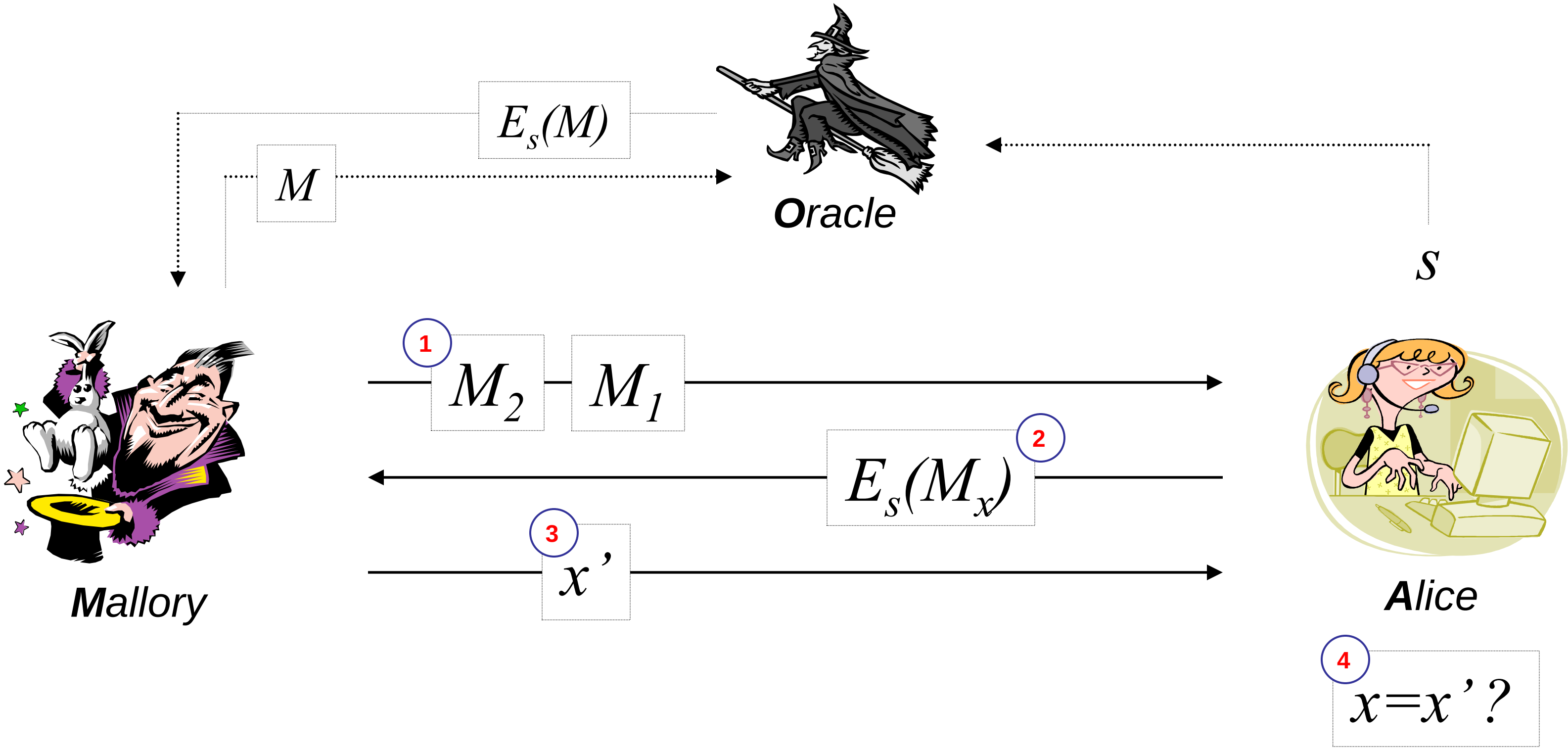
Semantic Security (==IND-CPA) Game

len(M1)=len(M2) ?



E() is **indistinguishable under a chosen plaintext attack** ("semantically secure") if no probabilistic polynomial time-bounded Mallory can succeed significantly better than guessing.

Semantic Security: extension to symmetric key



$E_s(M)$

M

Oracle

s

1 M_2 M_1

2 $E_s(M_x)$

3 x'

Mallory

Alice

4 $x=x'?$

Semantic Security: why do we care ?!

Deterministic, stateless schemes are insecure !

Semantic Security: why do we care ?!

Semantic security implies *bit security* !

Why/how (M_1=not(M_2))? Btw. what is bit security ? ☺

Examples

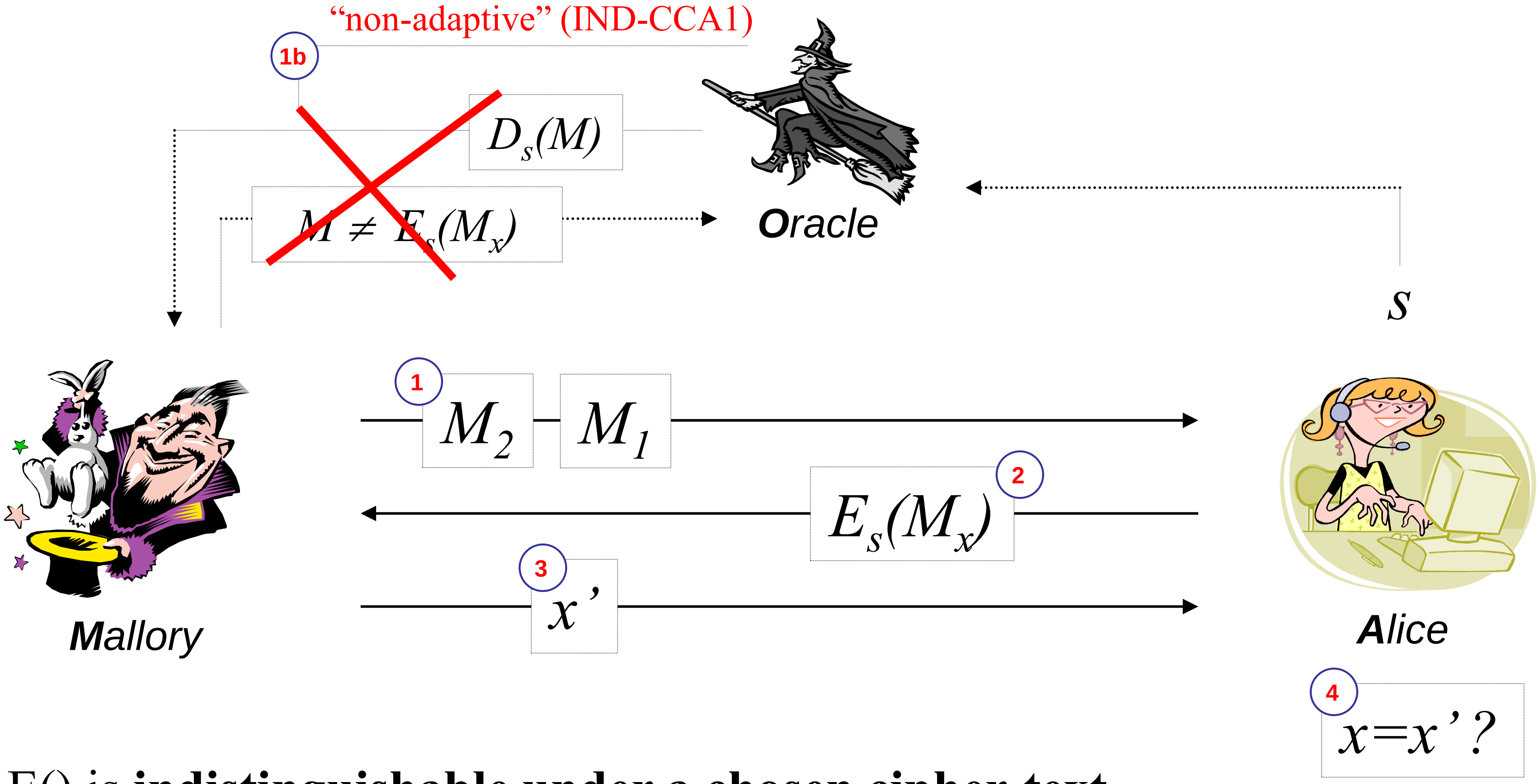
- RSA
  - non-semantically secure ! Why ?!
- RSA + padding (e.g., RSA-OAEP)
  - semantically secure
- Goldwasser Micali
  - semantically secure

Goldwasser-Micali Revisited

For each plaintext bit of “1” (respectively “0”) the ciphertext will contain a QR (respectively a QNR).

Key = knowledge of *p* and *q*

Variants: IND-CCA2 (adaptive)

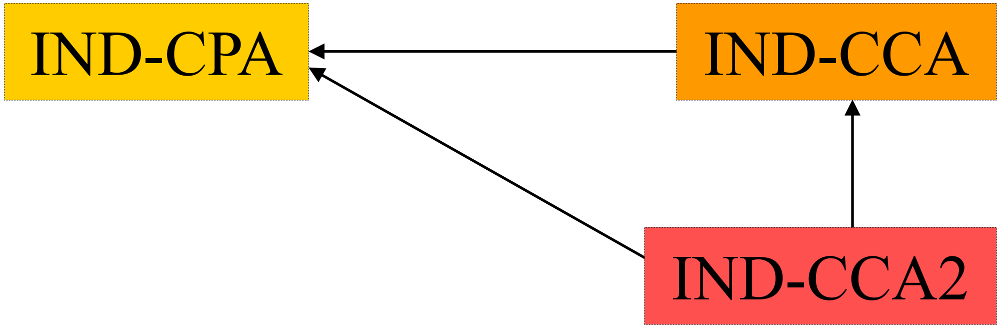


E() is **indistinguishable under a chosen cipher-text attack** if no probabilistic polynomial time-bounded Mallory can succeed significantly better than guessing.

IND-CCA: why do we care ?!

Adversary takes over equipment temporarily.

Relationships


IND-CPA
IND-CCA
IND-CCA2