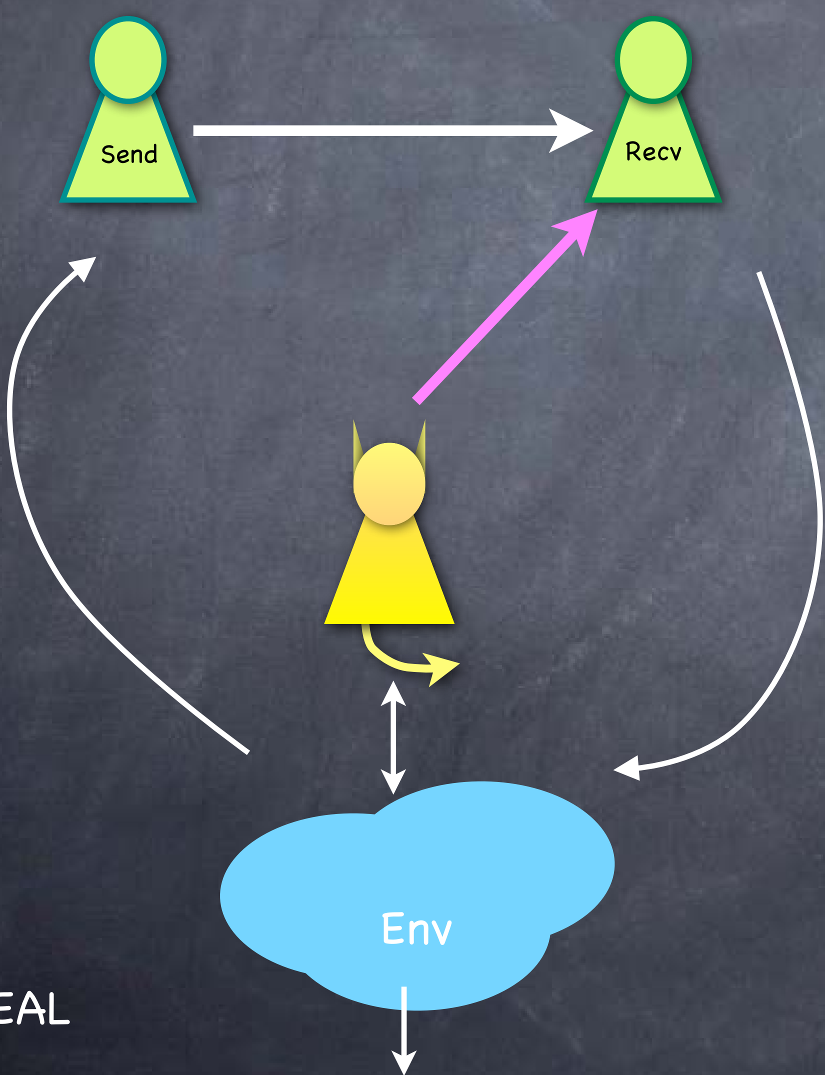
Public-Key Cryptography

Lecture 13

CCA Security (ctd.)

RECALL

SIM-CCA Security (PKE)



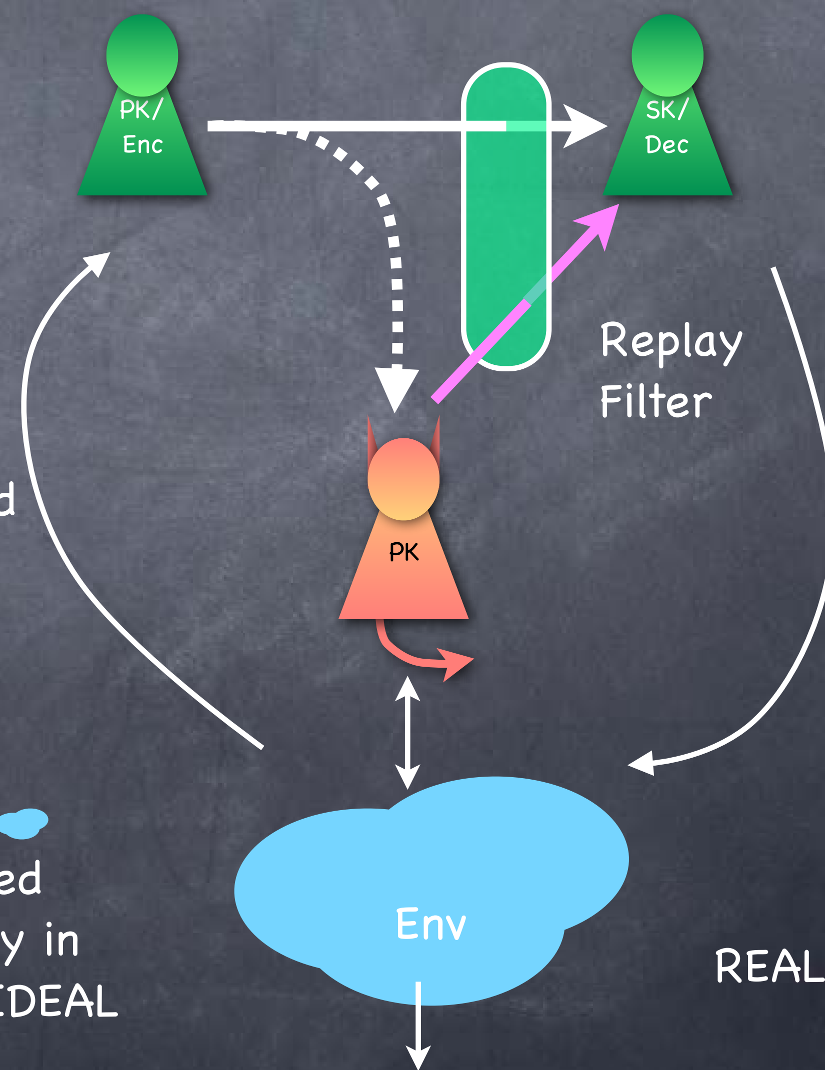
Secure (and correct) if:

∀

∃ s.t.

∀

output of
is distributed
≈ identically in
REAL and IDEAL



RECALL

CCA Secure PKE

- In SKE, to get CCA security, we used a MAC
  - Bob would accept only messages from Alice
- But in PKE, Bob <u>wants to</u> receive messages from Eve as well!
  - But only if it is indeed Eve's own message: she should know her own message!

RECALL

CCA Secure PKE Schemes

- Several schemes in the heuristic "Random Oracle Model"
  - RSA-OAEP
  - Fujisaki-Okamoto
  - DHIES (doesn't need the full power of ROM)
- Hybrid Encryption schemes: Improving the efficiency of PKE
- Today: Cramer-Shoup Encryption: A provably secure CCA scheme, under DDH assumption

CCA Secure PKE: Cramer-Shoup

- El Gamal-like: Based on DDH assumption
- Uses a prime-order group (e.g., $\mathbb{QR}_p^*$ for safe prime p)
- Enc(M) = (C,S)
  - $C = (g_1^x, g_2^x, MY^x)$ and $S = (WZ^{H(C)})^x$
  - g_1, g_2, Y, W, Z are part of PK
    - g_1, g_2 random generators, $Y=g_1^{y_1} g_2^{y_2}$, $W=g_1^{w_1} g_2^{w_2}$, $Z=g_1^{z_1} g_2^{z_2}$
      SK contains $(y_1,y_2,w_1,w_2,z_1,z_2)$
- Trapdoor: Using SK, and (g_1^x,g_2^x) can find Y^x, W^x, Z^x
  - If $a = g_1^x$ and $b = g_2^x$: $Y^x = a^{y_1}b^{y_2}$, $W^x = a^{w_1}b^{w_2}$, $Z^x = a^{z_1}b^{z_2}$
- Decryption: Compute Y^x, W^x, Z^x from C using SK.
  Check S and extract M.

H a "collision-resistant hash function" (Later)

Prime order group ⇒ all non-id elements are generators

Multiple SKs can explain the same PK (unlike El Gamal)

Proof Outline

- A hybrid where an "invalid encryption" is used for challenge:
  - Indistinguishable from valid encryption, under DDH assumption
  - It contains no information about the message (given just PK)
- But CCA adversary is not just given PK. Could she get information about the specific SK from decryption queries?
  - By querying decryption with only valid ciphertexts, adversary gets no information about SK (beyond given by PK)
  - Adversary can't create new "invalid ciphertexts" that get past the integrity check (except with negligible probability)
    - Relies on collision-resistance of H (used for efficiency)

Can replace H with an injective mapping to a pair of exponents, if longer keys and ciphertext can be used. But anyway assuming DDH, collision-resistance is easy (later).

Proof: Hybrid is Indistinguishable

- $C = (g_1^x, g_2^x, MY^x)$ and $S = (WZ^{H(C)})^x$ — With 1-negl probability, $x_1 \neq x_2$
  - $Y = g_1^{y_1} g_2^{y_2}$, $W = g_1^{w_1} g_2^{w_2}$, $Z = g_1^{z_1} g_2^{z_2}$
- **Hybrid experiment**: challenge ciphertext is prepared from random $g_1^{x_1}$ and $g_2^{x_2}$ and "Y^x, W^x, Z^x" computed using SK
- Indistinguishable from real experiment, by DDH (even given SK)
  - $(g_1, g_1^{x_1}, g_2, g_2^{x_2})$ where g_1,g_2 random generators (i.e., random, $\neq 1$):
    - If x_1, x_2 random, then (g, g^x, g^y, g^z) for random g,x,y,z.
    - If $x_1 = x_2 = x$, random, then (g, g^x, g^y, g^{xy}) for random g,x,y.
  - By DDH the two cases are indistinguishable (even given SK)

Proof: Hybrid has no Information

- $C = (g_1^x, g_2^x, MY^x)$ and $S = (WZ^{H(C)})^x$
  - $Y = g_1^{y_1} g_2^{y_2}$, $W = g_1^{w_1} g_2^{w_2}$, $Z = g_1^{z_1} g_2^{z_2}$
- Invalid ciphertext uses $x_1 \neq x_2$ and "Y^x, W^x, Z^x" computed using SK
- For invalid ciphertext, values of "Y^x, W^x, Z^x" will depend on the SK, and not just PK
  - e.g. "Y^x" $= a^{y_1}b^{y_2} = g_1^{(x_1-x_2)y_1} \cdot Y^{x_2}$ varies with SK if $x_1 \neq x_2$
  - Even if PK, x_1, x_2 are given, $g_1^{(x_1-x_2)y_1}$ is uniformly random
  - So an invalid challenge ciphertext (created using SK) is independent of the message, as "Y^x" is a one-time pad

Recall, only one challenge ciphertext in the IND-CCA experiment for PKE

Proof: Hybrid has no Information

- Remains to show that adversary (almost) never learns anything beyond PK about the keys
  - By querying decryption with only valid ciphertexts, adversary gets no information about SK beyond given by PK (decryption can be information-theoretically carried out using PK alone)
  - Adversary can't create new "invalid ciphertexts" that get past the integrity check (except with negligible probability)
    - Any invalid ciphertext with a new H(C) can fool at most a negligible fraction of the possible SKs: so the probability of adversary fooling the specific one used is negligible
    - Collision-resistance of H ⇒ same H(C) requires same C
    - And, same C requires same (C,S), since S is a deterministic function of C

Coming up

Proof: Invalid Ciphertexts Get Caught

- Claim: Even a computationally unbounded adversary can't create "invalid ciphertexts" (i.e., with $x_1 \neq x_2$) with H(C) different from that of the (invalid) challenge ciphertext, and get past the integrity check (except with negligible probability)
  - Working with exponents to the base g_1: let $g_2 = g_1^\alpha$, where $\alpha \neq 0$
    Public key has: (α, y, w, z), where $y = y_1 + \alpha y_2$, $w = w_1 + \alpha w_2$, $z = z_1 + \alpha z_2$
    Challenge ciphertext for message $M = g_1^\mu$ consists of
    x_1, αx_2, $c = \mu + x_1.y_1 + \alpha.x_2.y_2$, $s = (w_1 + \beta z_1)x_1 + \alpha(w_2 + \beta z_2)x_2$,
    where $\beta = H(\ (g_1^{x_1}, g_1^{\alpha.x_2}, g_1^c)\ )$
  - Claim: adversary can't find (x'_1, x'_2, β', s') with $x'_1 \neq x'_2$ and $\beta' \neq \beta$ and $s' = (w_1 + \beta' z_1)x'_1 + \alpha(w_2 + \beta' z_2)x'_2$
    - $s = (w + \beta z)x_1 + \alpha(w_2 + \beta z_2)(x_2 - x_1)$, where $x_2 - x_1 \neq 0$.
      So suppose we give $\gamma = (w_2 + \beta z_2)$ to the adversary (and μ, y_1, y_2).
    - $s' = (w + \beta' z)x'_1 + \alpha\gamma(x_2 - x_1) + \alpha(\beta' - \beta)z_2(x_2 - x_1)$
    - But z_2 is random (given the 3 linear equations for w, z, γ for the 4 variables $\{w_i, z_i \mid i \in \{1,2\}\ \}$), and hence there is negligible probability that candidate s' given by the adversary will be correct

Identity-Based Encryption

- In PKE, KeyGen produces a random (PK,SK) pair
- Can I have a "fancy public-key" (e.g., my name)?
  - No! Not secure if one can pick any PK and find an SK for it!
- But suppose a trusted authority for key generation
  - Then: Can it generate a valid (PK,SK) pair for any PK?
  - Identity-Based Encryption: a key-server (with a master secret-key) that can generate such pairs
    - Encryption will use the master public-key, and the receiver's "identity" (i.e., fancy public-key)
    - In PKE, sender has to retrieve PK for every party it wants to talk to (from a trusted public directory)
    - In IBE, receiver has to obtain its SK from the authority

Identity-Based Encryption

- Security requirement for IBE (will skip formal statement):
  - Environment/adversary decides the ID of the honest parties
  - Adversary can adaptively request SK for any number of IDs (which are not used for honest parties)
  - "Semantic security" for encryption with the ID of honest parties (i.e., with no access to decryption: CPA security)
- IBE (even CPA-secure) can easily give CCA-secure PKE!
  - IBE: Can't malleate ciphertext for one ID into one for another
  - $PKEnc_{MPK}(m) = (id, C=IBEnc_{MPK}(id; m), sign_{id}(C))$
  - Security: can't create a different encryption with same id (signature's security); can't malleate using a different id (IBE's security)

Digital Signature with its public-key used as the ID in IBE

Today

- CCA secure PKE
    - Cramer-Shoup Encryption
- Identity Based Encryption
- Next up: Hash functions, Digital Signatures