Public-Key Cryptography

Lecture 12

CCA Security

CCA Secure PKE

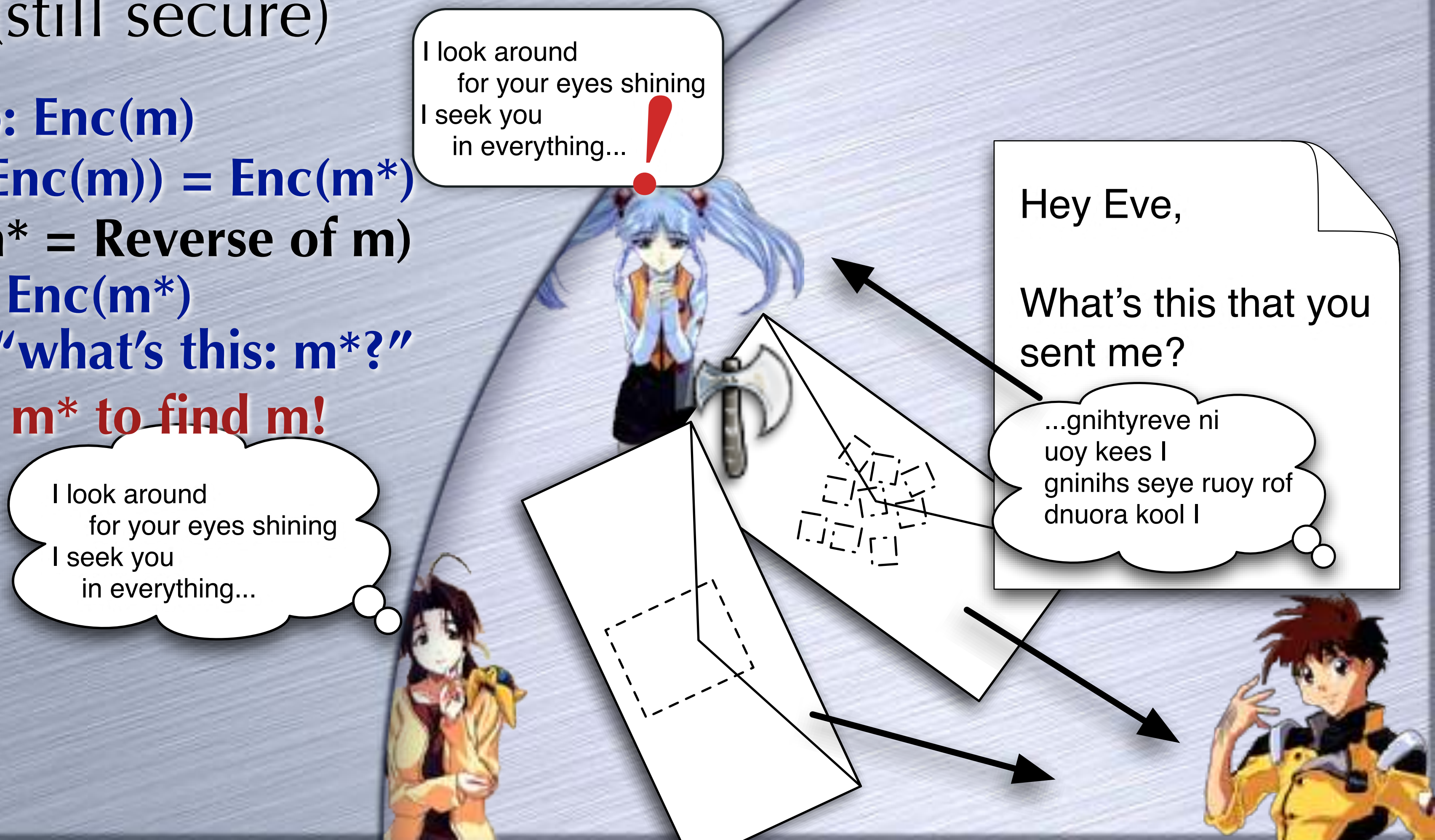
- In SKE, to get CCA security, we used a MAC
  - Bob would accept only messages from Alice
- But in PKE, Bob wants to receive messages from Eve as well!
  - But only if it is indeed Eve's own message: she should know her own message!

Chosen Ciphertext Attack

- Suppose Enc SIM-CPA secure
  - Suppose encrypts a character at a time (still secure)

A subtle
e-mail attack

Alice → Bob: Enc(m)
Eve: Hack(Enc(m)) = Enc(m*)
(where m* = Reverse of m)
Eve → Bob: Enc(m*)
Bob → Eve: "what's this: m*?"
Eve: Reverse m* to find m!



Malleability

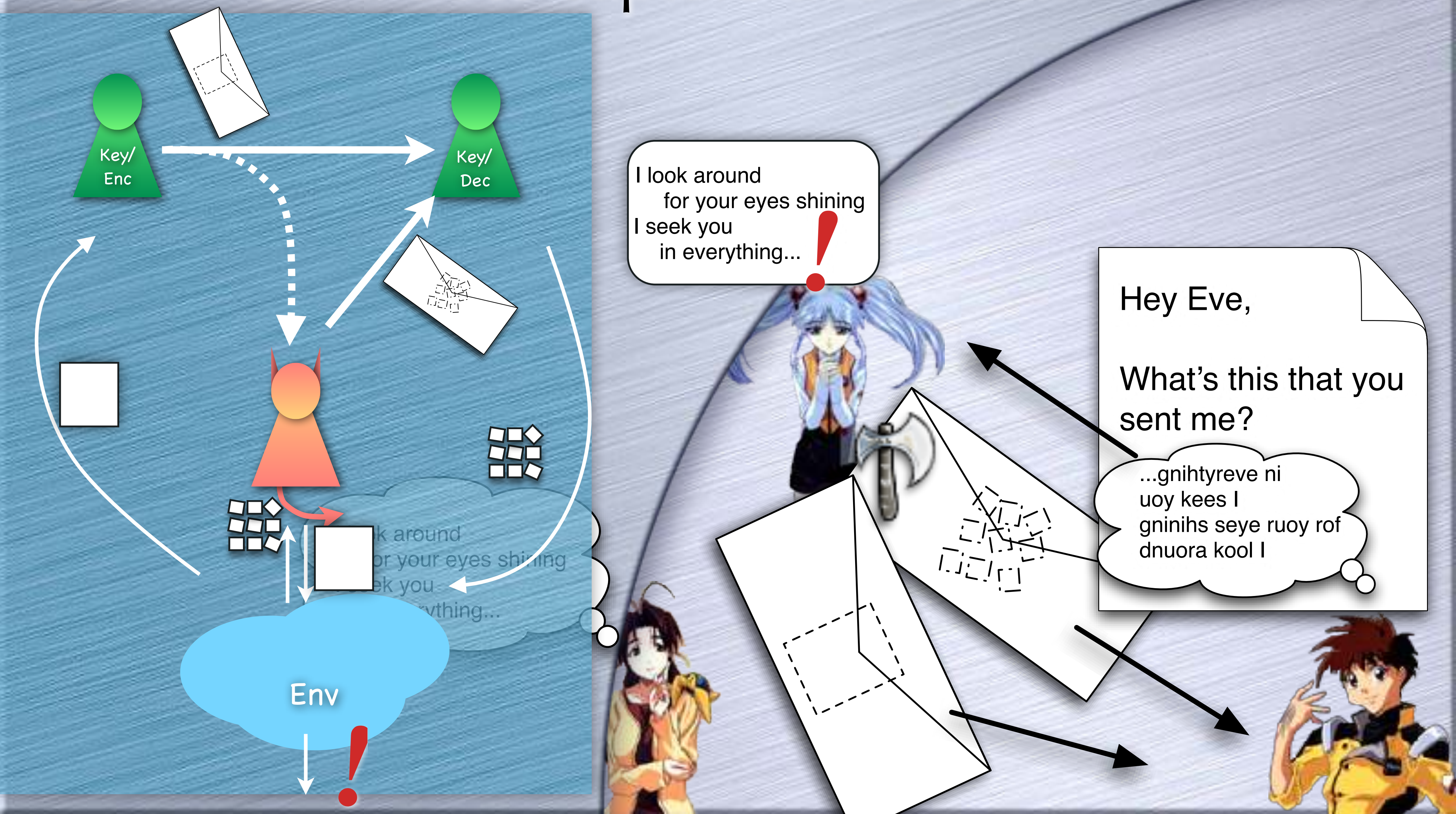
- Malleability: Eve can "malleate" a ciphertext (without having to decrypt it) to produce a new ciphertext that would decrypt to a "related" message

More subtly, the 1 bit - valid or invalid - may leak information on message or SK

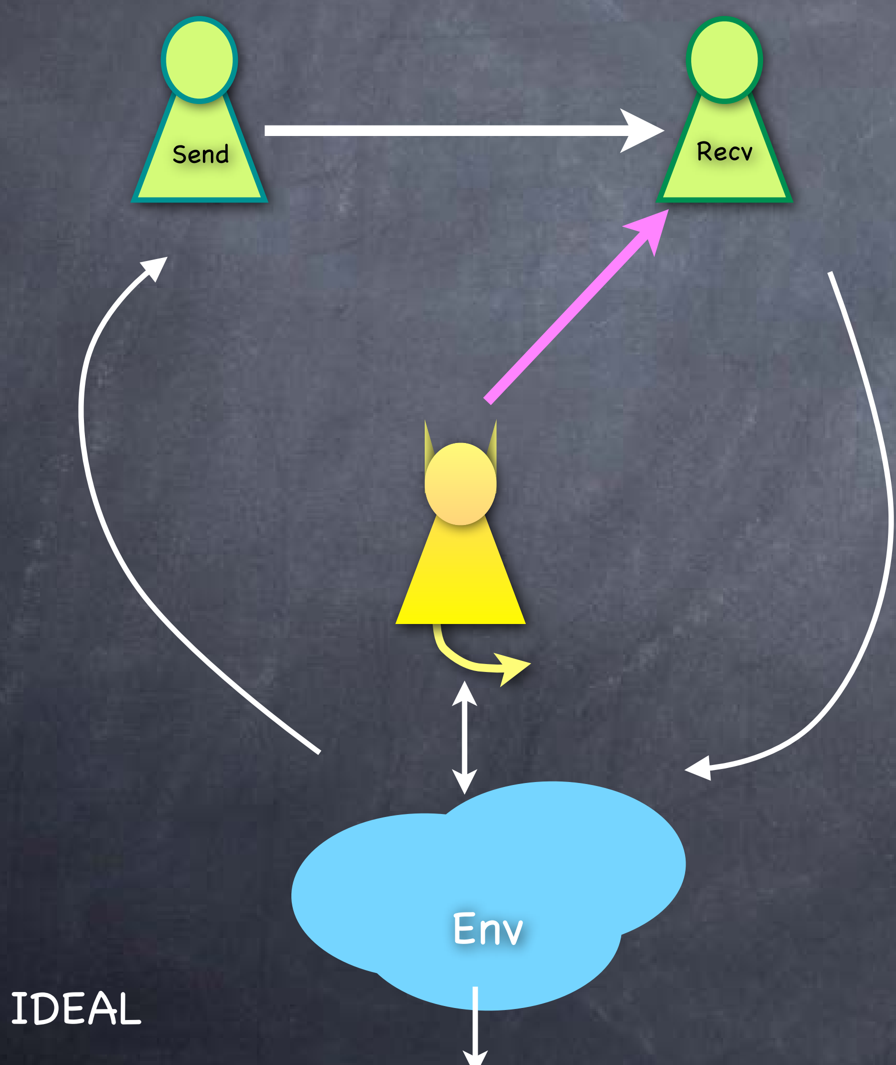
- E.g.: Malleability of El Gamal
  - Recall: $Enc_{(G,g,Y)}(m) = (g^x, M.Y^x)$
  - Given (X,C) change it to (X,TC): will decrypt to TM
  - Or change (X,C) to (X^a,C^a): will decrypt to M^a
- If chosen-ciphertext attack possible
  - i.e., Eve can get a ciphertext of her choice decrypted
  - Then Eve can exploit malleability to learn something "related to" Alice's messages

Chosen Ciphertext Attack

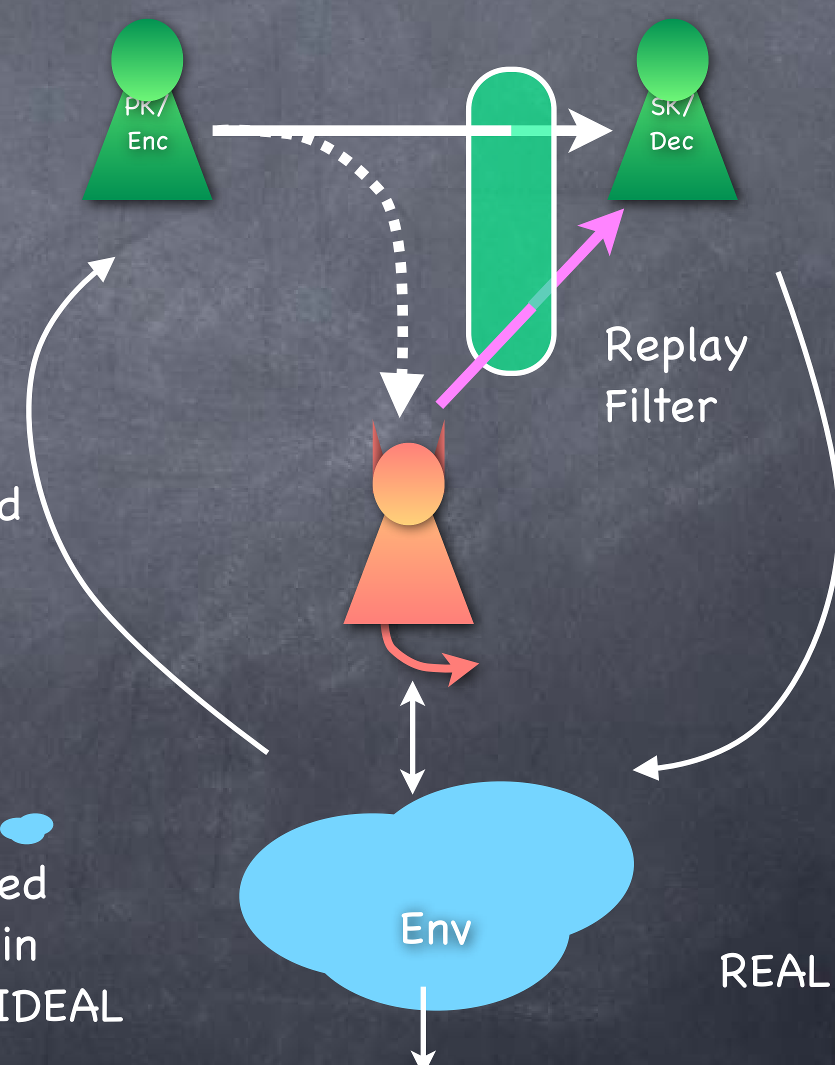
- SIM-CCA: does capture this attack



SIM-CCA Security (PKE)



Secure (and correct) if:
∀
∃ s.t.
∀
output of
is distributed identically in REAL and IDEAL



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)
- Uses a collision-resistant hash function inside an "integrity tag"
  - Enc(M) = (C,S)

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

    - $C = (g_1^x, g_2^x, MY^x)$ and $S = (WZ^{H(C)})^x$
    - g_1, g_2, Y, W, Z are part of PK
      - $Y = g_1^{y1} g_2^{y2}$, $W = g_1^{w1} g_2^{w2}$, $Z = g_1^{z1} g_2^{z2}$. SK contains $(y_1,y_2,w_1,w_2,z_1,z_2)$

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

  - Trapdoor: Using SK, and (g_1^x,g_2^x) can find Y^x, W^x, Z^x
    - If (g_1^{x1},g_2^{x2}), $x_1 \neq x_2$, then "Y^x, W^x, Z^x" vary with different SKs
  - Decryption: Check S (assuming $x_1=x_2$) and extract M

Security of CS Scheme: Proof Sketch

$(g_1, g_1^{x1}, g_2, g_2^{x2})$ is of the form (g, g^x, g^y, g^{xy}) iff $x_1 = x_2$

- An "invalid encryption" can be used for challenge such that
  - It contains no information about the message (given just PK)
  - Is indistinguishable from valid encryption, under DDH assumption
- 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)
    - 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 ⇒ new C will lead to new H(C)

More details

- 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, $y = y_1 + \alpha y_2$, $w = w_1 + \alpha w_2$, $z = z_1 + \alpha z_2$
    Challenge ciphertext has x_1, x_2, $s = (w_1 + \beta z_1)x_1 + \alpha(w_2 + \beta z_2)x_2$
    where $\beta = H((g_1^{x1}, g_1^{\alpha.x2}, M.(g_1^{x1.y1 + \alpha.x2.y2})))$
  - Claim: adversary can't find $s' = (w_1 + \beta' z_1)x'_1 + \alpha(w_2 + \beta' z_2)x'_2$ with $x'_1 \neq x'_2$ and $\beta' \neq \beta$
    - $s = (w + \beta z)x_1 + \alpha(w_2 + \beta z_2)(x_2 - x_1)$, where $x_2 - x_1 \neq 0$.
      So suppose we give $\gamma = (w_2 + \beta z_2)$ to the adversary.
    - $s' = (w + \beta' z)x'_1 + \alpha\gamma(x_2 - x_1) + \alpha(\beta' - \beta)z_2(x_2 - x_1)$
    - But z_2 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 s' given by the adversary will match the correct z_2