Public-Key Cryptography

Lecture 13

CCA Security

Hybrid Encryption

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 wants to 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: 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

Another CCA Secure PKE: RSA-OAEP

- RSA-OAEP
  - "Text-book RSA encryption" (i.e., f_{RSA}, the Trapdoor OWP candidate) applied to an "encoding" of the message
    - Encoding is randomized
    - Encoding uses a hash function modeled as a "Random Oracle"
    - Security in the RO Model, assuming f_{RSA} a OWP
  - Part of RSA Cryptography Standard (PKCS#1 Ver 2.1). Commonly used in SSL/TLS implementations

Random Oracle Model

- Random Oracle: a mythical oracle that, when initialized, picks a random function $R:\{0,1\}^* \to \{0,1\}^{n(k)}$ and when queried with x, returns R(x)
    - All parties have access to the same RO
- In ROM, evaluating some "hash function" H would be modeled as accessing an RO
    - Hope: the code for H has "no simple structure" and only way to get anything useful from it is to evaluate it on an input
- Sometimes security definitions need to be adapted for ROM
- Rigorous proofs of security, <u>after</u> moving to the ROM

Random Oracle Model

- **There is no Pseudo-RO**
  - Unlike PRF, RO must be locally evaluable for all parties. (think: giving out the seed of a PRF)
- There are schemes secure in ROM, such that for any instantiation of the RO, the scheme is insecure!
  - Also natural constructs/primitives which are realizable in ROM, but not in the standard model!
- What does a proof in ROM tell us?
  - Secure against attacks that treat H as a blackbox (and for which H is pseudorandom)

Hybrid Encryption

- PKE is far less efficient compared to SKE (even in ROM)
  - SKE using Block Ciphers (e.g. AES) and MAC is very fast
  - RSA-OAEP uses modular exponentiations (Cramer-Shoup even more)
- Hybrid encryption: Use (CCA secure) PKE to transfer a key for the (CCA secure) SKE. Use SKE with this key for sending data
  - Hopefully the combination remains CCA secure
  - Note: PKE used to encrypt only a (short) key for the SKE
    - Relatively low overhead on top of the (fast) SKE encryption

Hybrid Encryption

Or to generate a key

- Hybrid Encryption: KEM/DEM paradigm
  - Key Encapsulation Method: a public-key scheme to transfer a key
  - Data Encapsulation Method: a symmetric-key scheme (using the key transferred using KEM)
- For what KEM/DEM is a hybrid encryption scheme CCA secure?
  - Works if KEM is a SIM-CCA secure PKE scheme and DEM is a SIM-CCA secure SKE scheme
    - Easy to prove using "composition" properties of the SIM definition
  - Less security sufficient: KEM used to transfer a random key; DEM uses a new key every time.

CCA Secure PKE: DHIES

- Diffie-Hellman Integrated Encryption Scheme
  - Part of some standards
- Essentially a hybrid scheme
  - Data Encapsulation: CPA secure SKE, and MAC
  - Key Encapsulation: $X=g^x$. Let $K=Y^x$, where Y is the PK (as in El Gamal), and (K_{SKE},K_{MAC}) = Hash(K) (where $K=Y^x=X^y$)
- CCA security based on a complex (non-standard) assumption involving Hash and the group: "Oracle Diffie-Hellman Assumption"

Another PKE Scheme: CCA Secure in RO Model

- Fujisaki-Okamoto Hybrid scheme
  - KEM encrypts random x, using random coins derived as H(m,x), where m is the message and H a "random oracle"
  - DEM encrypts m with key K = G(x), where G is another "random oracle"
  - Decryption decrypts x, then m, and then checks if KEM was correct
  - Very weak security sufficient for encryptions used in KEM and DEM (but only with H, G modelled as random oracles)

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
  - $\text{PKEnc}_{\text{MPK}}(m) = (\text{id}, C=\text{IBEnc}_{\text{MPK}}(\text{id}; m), \text{sign}_{\text{id}}(C))$
  - 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
  - Hybrid Encryption: KEM/DEM
    - e.g., DHIES
  - In Random Oracle Model
    - e.g. RSA-OAEP, Fujisaki-Okamoto
  - From Identity Based Encryption
- Next up: Hash functions, Digital Signatures