COL759:
CRYPTOGRAPHY AND COMPUTER SECURITY

2022-23 (SEMESTER 1)

LECTURE 33: RANDOM ORACLE REVIEW, CCA SECURITY

RANDOM ORACLES REVIEW

- Almost all real-world cryptosystems use heuristics. Heuristics like complex hash functions, permutations etc.

- Security is proven in 'idealised models'. Random oracle model is one such idealised model. Other idealised models: the ideal cipher model, the generic group model, etc.

- Random oracle model:
  - Propose scheme using a function H
  - Proof of security is in random oracle model, where challenger chooses a random function for H, adversary must query the challenger for eval. of H

RANDOM ORACLES REVIEW

- Proof in Random Oracle model $\not\Longrightarrow$ proof in std. model
- Random oracle model proof techniques:
  - CRHFs/MACs: fresh output for every new input
  - RSA-based encryption: fresh output for every new input
    Challenger *sees* random oracle queries made by adversary

TODAY'S LECTURE

- Random oracle model proof techniques:
  - Security against chosen ciphertext attacks
  - A new random oracle model proof technique

ENCRYPTION SCHEMES SEEN SO FAR

ELGAMAL

- Public key: (g, g^a)

- Message space: prime order group $\mathbb{G}$

Enc(m, pk): $(g^b, m \cdot g^{ab})$

How to encrypt longer messages?

$$\text{Enc}\left(m = (m_1, \ldots, m_\ell), \text{pk} = (g, g^a)\right) = \left(g^{b_1}, m_1 \cdot g^{ab_1}, \ldots, g^{b_\ell}, m_\ell \cdot g^{ab_\ell}\right)$$

Where $b_1, \ldots, b_\ell$ are chosen at random

We cannot repeat the same $b_i s$

ENCRYPTION SCHEMES SEEN SO FAR

ELGAMAL

- Public key: (g, g^a)

- Message space: prime order group $\mathbb{G}$

Enc(m, pk): $(g^b, m \cdot g^{ab})$

Is the scheme malleable?

Given encryption of m, we can produce encryption of $\alpha \cdot m$ for any $\alpha \in \mathbb{G}$

ENCRYPTION SCHEMES SEEN SO FAR

RSA-HEURISTIC

- Public key: (N, e)

- Message space: $\{0,1\}^*$

Enc(m, pk): $\left(x^e, \mathsf{Enc}_{\mathrm{sym}}(m, H(x)) \right)$

Is the scheme malleable?

Depends on $\mathsf{Enc}_{\mathrm{sym}}$. E.g.: if Shannon OTP is used, then this is malleable.

HOW TO HANDLE MALLEABILITY ATTACKS ?

Symmetric Key Encryption:
Malleability attacks prevented using authenticated encryption

Public Key Encryption with Ciphertext Integrity?

Ciphertext integrity is not possible in PKE setting

Security against Chosen Ciphertext Attacks?

SECURITY AGAINST CHOSEN CIPHERTEXT ATTACKS (CCA SECURITY)

Chall.		Adv.	
Chooses (pk, sk), bit b	pk $\rightarrow$		Setup
$y_i = \mathrm{Dec}(\mathrm{ct}_i, sk)$	$\leftarrow$ Decrypt ct_i y_i $\rightarrow$		Pre-chall. dec. queries
$\mathrm{ct}^* \leftarrow \mathrm{Enc}(\mathrm{m}_b^*, pk)$	$\leftarrow$ m_0^* m_1^* ct^* $\rightarrow$		Chall.
$y_i = \mathrm{Dec}(\mathrm{ct}_i, sk)$	$\leftarrow$ Decrypt ct_i ($\neq \mathrm{ct}^*$) y_i $\rightarrow$		Post-chall. queries
	$\leftarrow$ b′		Guess

A WEAKER NOTION (CCA-1 SECURITY)

Chall. Adv.

Chooses (pk, sk), bit b — Setup

Pre-chall. dec. queries:

Decrypt ct_i ←

$y_i = \mathrm{Dec}(ct_i, sk)$

y_i →

Chall.:

$m_0^* \quad m_1^*$ ←

$ct^* \leftarrow \mathrm{Enc}(m_b^*, pk)$

ct^* →

Guess:

b′ ←

CCA-1 does not prevent malleability attacks. But it is a useful notion to study, especially as a stepping stone for building CCA secure encryption. Also captures 'lunchtime attacks'.

SECURITY AGAINST CHOSEN CIPHERTEXT ATTACKS (CCA SECURITY)

Which of the following schemes is not CCA secure?

Elgamal : Not CCA

RSA-heuristic : May not be CCA, depends on base encryption scheme

SECURITY AGAINST CHOSEN CIPHERTEXT ATTACKS (CCA SECURITY)

Which of the following schemes is not CCA-1 secure?

Elgamal : no CCA-1 attack known

RSA-heuristic : depends on base encryption scheme
there exist contrived base schemes which will result in a CCA-1 attack

CONSTRUCTING CCA SECURE PKE : ENCRYPT-THEN-MAC ?

Encrypt-then-MAC works in the symmetric key setting, but does not work in the public key setting.

The first obstacle is that MAC is a private key primitive. However, suppose we use the public-key variant of MACs (these are called digital signature schemes). In a digital signature scheme, the setup algorithm outputs a secret signing key together with a public verification key. Only the person holding the signature key can sign on a message, but anyone can verify the signature using a verification key. Security states that, given a verification key, one cannot produce a signature forgery, even after seeing many signatures.

Suppose you are given a semantically secure encryption scheme (Enc, Dec), and a signature scheme (Sign, Verify).

A natural idea to build a CCA-secure encryption scheme is the following:
To encrypt m, first compute ct = Enc(m, pk). Then choose signing keys (sk, vk).
Compute signature on ct using sk. Finally, send (ct, signature, vk) as the ciphertext.

This is NOT CCA secure. (Why?)
Hint: given a challenge cipher text, the adversary can replace the verification key with a different vk, and send a fresh decryption query.

A BRIEF HISTORY OF CCA SECURITY

SCHEME 1

- Public key: (N, e), $N \approx 2^{\ell}$
- Message space: $\{0,1\}^{\ell/2}$

  Enc(m, pk): $(r \mid\mid m)^e$

SCHEME 2

- Public key: (N, e), $N \approx 2^{\ell}$
- Message space: $\{0,1\}^*$

  Enc(m, pk): $\left(x^e, Enc_{sym}(m, H(x))\right)$

1989 / 90 [SR, NY] — Definition of CCA proposed

1993 — Public Key Cryptography Standards (PKCS) proposed by RSA Labs

Used (variant of) Scheme 1

1994 [BR] — Random Oracle Model proposed

Scheme 2 with auth. enc. scheme Enc_{sym} proven CCA secure in RO model

1995 [BR] — More efficient heuristic construction (OAEP), with CCA security in RO model

text-aware encryption, which we introduce here. This new implies "ambitious" goals like chosen-ciphertext security

1998 [B] — Real world CCA attack

1999 — PKCS updated to use OAEP

(Widely used in practice currently, might become obsolete when we switch to post-quantum crypto systems)

1999 [FO] — Heuristic scheme that transforms any semantic secure scheme to CCA secure in RO model

(Most post-quantum candidates use this transformation)

ADDITIONAL REFERENCES

[SR]: Simon, Rackoff: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack.

[NY]: Naor, Yung: Public key cryptosystems provably secure against chosen ciphertext attacks.

[BR94]: Bellare, Rogaway: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols

[BR95]: Bellare, Rogaway: Optimal Asymmetric Encryption - How to Encrypt with RSA

[B]: Bleichenbacher: Chosen Ciphertext Attacks against Protocols Based on RSA Encryption Standard PKCS #1.

[FO]: Fujisaki, Okamoto. Secure integration of asymmetric and symmetric encryption schemes

THANKS!