# EECS 575: Advanced Cryptography
# Fall 2022
# Lecture 17

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Announcements

- HW4 is out, due 11/7
- Alexandra's office hours are cancelled this week
  - My extra OH will be Thursday 11/3, 11am-noon
- Post on Piazza

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Public-Key Encryption

- IND-CPA security for PKE
- ElGamal - cyclic group with DDH hard

$G$ $\langle g \rangle$ $\text{ord}(G) = q$

$a, b, c \leftarrow \mathbb{Z}_q$

$(g, g^a, g^b, g^{ab}) \approx_c (g, g^a, g^b, g^c)$

# Public-Key Encryption

$\mathbb{G}, \langle g \rangle, \text{ord}(q)$

- Gen: $a \leftarrow \mathbb{Z}_q$, Ret $(g^a, a)$
- Enc(pk, m): $r \leftarrow \mathbb{Z}_q$, Ret $(g^r, (pk)^r \cdot m)$
- Dec(sk, $(c_0, c_1)$): Ret $c_1 / (c_0)^{sk}$

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Hybrid Public-Key Encryption

PKE is slow (≈1000x slowdown).

" has large ciphertexts

Instead of encrypting message with PKE, encrypt symmetric key. Use SKE to encrypt

"key encapsulation mechanism"

KEM - NIST PQC

# Hybrid Public-Key Encryption

$PKE = (PGen, PEnc, PDec)$

$SKE = (SGen, SEnc, SDec)$

- $Gen$: $(pk, sk) \leftarrow PGen$, Ret $(pk, sk)$
- $Enc(pk, m)$:
  - $k \leftarrow SGen$ $|k| = \lambda$
  - $c_0 \leftarrow PEnc(pk, k)$ ← short/small
  - $c_1 \leftarrow SEnc(k, m)$
  - Ret $(c_0, c_1)$ $\leq poly(\lambda)$
- $Dec(sk, (c_0, c_1))$:
  - $k = PDec(sk, c_0)$
  - $m = SDec(k, c_1)$
  - Ret $m$

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Hybrid encryption analysis

**Thm:** If PKE and SKE are IND-CPA, then HE[PKE, SKE] is IND-CPA.

**Proof:** (Sketch):

$H_0$: oracle is HE, encrypts $m_0$

IND-CPA of PKE

$H_1$: oracle is HE except $c_0 \leftarrow \text{Enc}(pk, 0)$

IND-CPA of SKE

$H_2$: oracle is HE except $c_0 \leftarrow \text{Enc}(pk, 0)$ and encrypts $m_1$

IND-CPA of PKE

$H_3$: oracle is HE, encrypts $m_1$

# Hybrid encryption analysis

$|\Pr[H_0^{\mathcal{A}}=1] - \Pr[H_1^{\mathcal{A}}=1]| \leq \mathrm{Adv}^{\mathrm{IND\text{-}CPA}}(\mathcal{B})$

$\mathcal{B}$ returns $\mathrm{Enc}(pk, m_0)$ or $\mathrm{Enc}(pk, m_1)$

$\mathrm{IND\text{-}CPA}^{\mathcal{A}}_0$:
$(pk, sk) \leftarrow \mathrm{PKE.Gen}$
$b \leftarrow \mathcal{A}^{C_0(\cdot,\cdot)}(pk)$

$C_0(m_0, m_1)$:
Ret $\mathrm{PKE.Enc}(pk, m_0)$

$\mathrm{IND\text{-}CPA}^{\mathcal{A}}_1$:
$(pk, sk) \leftarrow \mathrm{PKE.Gen}$
$b \leftarrow \mathcal{A}^{C_1(\cdot,\cdot)}(pk)$

$C_1(m_0, m_1)$:
Ret $\mathrm{PKE.Enc}(pk, m_1)$

$H_0^{\mathcal{A}}$ $\mathrm{HE}[\mathrm{PKE}, \mathrm{SKE}]$:
$pk, sk \leftarrow \mathrm{PGen}$
$b \leftarrow \mathcal{A}^{\Phi_0(\cdot,\cdot)}(pk)$

$\Phi_0(m_0, m_1)$:
$k \leftarrow \mathrm{SGen}$
$c_0 \leftarrow \mathrm{PEnc}(pk, k)$
$c_1 \leftarrow \mathrm{SEnc}(k, m_0)$
Ret $(c_0, c_1)$

$H_1^{\mathcal{A}}$ $\mathrm{HE}[\mathrm{PKE}, \mathrm{SKE}]$:
$pk, sk \leftarrow \mathrm{PGen}$
$b \leftarrow \mathcal{A}^{\Phi_0(\cdot,\cdot)}(pk)$

$\Phi_0(m_0, m_1)$:
$k \leftarrow \mathrm{SGen}$
$c_0 \leftarrow \mathrm{PEnc}(pk, 0)$
$c_1 \leftarrow \mathrm{SEnc}(k, m_0)$
Ret $(c_0, c_1)$

$\mathcal{B}^{\Phi(\cdot,\cdot)}(pk)$:
$\Phi_0(m_0, m_1)$
$b \leftarrow \mathcal{A}^{(pk)}$
Ret $b$

$\hat{\Phi}_0(m_0, m_1)$:
$k \leftarrow \mathrm{SGen}$
$c_0 = \Phi(k, 0)$
$c_1 \leftarrow \mathrm{SEnc}(k, m_0)$
Ret $(c_0, c_1)$

# Hybrid encryption analysis

$\mathrm{IND\text{-}CPA}^{\mathcal{A}}_0$:
$(pk, sk) \leftarrow \mathrm{PKE.Gen}$
$b \leftarrow \mathcal{A}^{C_0(\cdot,\cdot)}(pk)$

$C_0(m_0, m_1)$:
Ret $\mathrm{PKE.Enc}(pk, m_0)$

$\mathrm{IND\text{-}CPA}^{\mathcal{A}}_1$:
$(pk, sk) \leftarrow \mathrm{PKE.Gen}$
$b \leftarrow \mathcal{A}^{C_1(\cdot,\cdot)}(pk)$

$C_1(m_0, m_1)$:
Ret $\mathrm{PKE.Enc}(pk, m_1)$

$$\left|\Pr[H_1^{\mathcal{A}} = 1] - \Pr[H_2^{\mathcal{A}} = 1]\right| \le \mathrm{Adv}^{\mathrm{INDCPA}}(\mathcal{B})$$

$H_1^{\mathcal{A}}$ $HE[PKE, SKE]$:

$pk, sk \leftarrow \mathrm{PGen}$
$b \leftarrow \mathcal{A}^{\Phi_0(\cdot,\cdot)}(pk)$

$\Phi_0(m_0, m_1)$:

$k \leftarrow \mathrm{SGen}$
$c_0 \leftarrow \mathrm{PEnc}(pk, 0)$
$c_1 \leftarrow \mathrm{SEnc}(k, m_0)$ //
Ret $(c_0, c_1)$

$H_2^{\mathcal{A}}$ $HE[PKE, SKE]$:

$pk, sk \leftarrow \mathrm{PGen}$
$b \leftarrow \mathcal{A}^{\Phi_1(\cdot,\cdot)}(pk)$

$\Phi_1(m_0, m_1)$:

$k \leftarrow \mathrm{SGen}$
$c_0 \leftarrow \mathrm{PEnc}(pk, 0)$
$c_1 \leftarrow \mathrm{SEnc}(k, m_1)$ //
Ret $(c_0, c_1)$

$\mathcal{B}$

$(pk, sk) \leftarrow \mathrm{PGen}$
$b \leftarrow \mathcal{A}^{\tilde{\Phi}(\cdot,\cdot)}(pk)$
Ret $b$

$\tilde{\Phi}(m_0, m_1)$:

$c_0 \leftarrow \mathrm{PEnc}(pk, 0)$
$c_1 = \Phi(m_0, m_1)$
Ret $(c_0, c_1)$ //

# Hybrid encryption analysis

$\text{IND-CPA}^A_0$:
$(pk, sk) \leftarrow \text{PKE.Gen}$
$b \leftarrow A^{C_0(\cdot,\cdot)}(pk)$

$C_0(m_0, m_1)$:
Ret $\text{PKE.Enc}(pk, m_0)$

$\text{IND-CPA}^A_1$:
$(pk, sk) \leftarrow \text{PKE.Gen}$
$b \leftarrow A^{C_1(\cdot,\cdot)}(pk)$

$C_1(m_0, m_1)$:
Ret $\text{PKE.Enc}(pk, m_1)$

Exercise: $G_0$ $H_2 \rightarrow H_3$ via similar argument.

$H_1^A\,[HE[PKE, SKE]]$:

$pk, sk \leftarrow \text{PGen}$
$b \leftarrow A^{\phi_0(\cdot,\cdot)}(pk)$

$\phi_0(m_0, m_1)$:
$k \leftarrow \text{SGen}$
$c_0 \leftarrow \text{PEnc}(pk, 0)$
$c_1 \leftarrow \text{SEnc}(k, m_0)$ //
Ret $(c_0, c_1)$

$H_2^A\,[HE[PKE, SKE]]$:

$pk, sk \leftarrow \text{PGen}$
$b \leftarrow A^{\phi_1(\cdot,\cdot)}(pk)$

$\phi_1(m_0, m_1)$:
$k \leftarrow \text{SGen}$
$c_0 \leftarrow \text{PEnc}(pk, 0)$
$c_1 \leftarrow \text{SEnc}(k, m_1)$ //
Ret $(c_0, c_1)$

$H_3^A\,[HE[PKE, SKE]]$:

$pk, sk \leftarrow \text{PGen}$
$b \leftarrow A^{\phi_1(\cdot,\cdot)}(pk)$

$\phi_1(m_0, m_1)$:
$k \leftarrow \text{SGen}$
$c_0 \leftarrow \text{PEnc}(pk, k)$
$c_1 \leftarrow \text{SEnc}(k, m_1)$ //
Ret $(c_0, c_1)$

# Agenda for this lecture

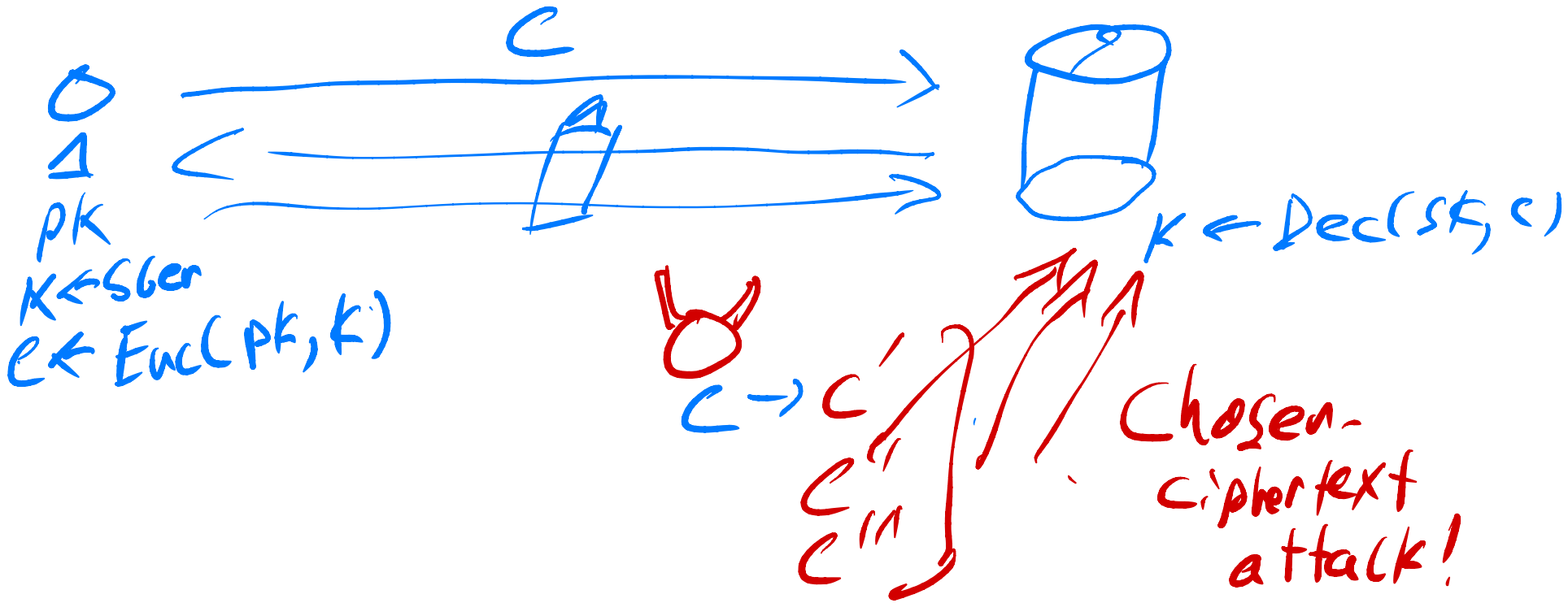
- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Chosen-ciphertext attacks on PKE

Late 90s : SSL widespread

Are CCAs feasible?

Bleichenbacher : million-message attack



# Chosen-ciphertext attacks on PKE

$\underline{IND\text{-}CCA0^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow Gen$; $c^* = \perp$

$b \leftarrow \mathcal{A}^{\mathcal{E}_0(\cdot,\cdot), Dec(\cdot)}(pk)$

$\underline{\mathcal{E}_0(m_0, m_1)}$:

$c^* \leftarrow Enc(pk, m_0)$

Ret $c^*$

$\underline{Dec(c)}$:

IF $c \neq c^*$: Ret $Dec(sk, c)$

$\underline{IND\text{-}CCA1^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow Gen$; $c^* = \perp$

$b \leftarrow \mathcal{A}^{\mathcal{E}_1(\cdot,\cdot), Dec(\cdot)}(pk)$

$\underline{\mathcal{E}_1(m_0, m_1)}$:

$c^* \leftarrow Enc(pk, m_1)$

Ret $c^*$

$\underline{Dec(c)}$:

IF $c \neq c^*$: Ret $Dec(sk, c)$

# Chosen-ciphertext attacks on PKE

$\underline{IND\text{-}CCA0^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow Gen$; $c^* = \perp$

$b \leftarrow \mathcal{A}^{C_0(\cdot,\cdot), Dec(\cdot)}(pk)$

$\underline{C_0(m_0, m_1)}$:

$c^* \leftarrow Enc(pk, m_0)$

Ret $c^*$

$\underline{Dec(c)}$:

IF $c \neq c^*$: Ret $Dec(sk, c)$

$\underline{IND\text{-}CCA1^{\mathcal{A}}_{PKE}}$:

$(pk, sk) \leftarrow Gen$; $c^* = \perp$

$b \leftarrow \mathcal{A}^{C_1(\cdot,\cdot), Dec(\cdot)}(pk)$

$\underline{C_1(m_0, m_1)}$:

$c^* \leftarrow Enc(pk, m_1)$

Ret $c^*$

$\underline{Dec(c)}$:

IF $c \neq c^*$: Ret $Dec(sk, c)$

**Thm**: **E/Gamal** **is not** IND-CCA

**Proof**:

$\underline{\mathcal{B}^{CC(\cdot,\cdot), Dec(\cdot)}(pk)}$:

$(C_0, C_1) = CC(m_0, m_1)$

$c^* = (C_0, C_1 \cdot m^*)$

$m' = Dec(c^*)$

If $m'/m_0 = m^*$ Ret 0

Else Ret 1

**E/Gamal**:

$G, \langle g \rangle, ord(q)$

- Gen: $a \leftarrow \mathbb{Z}_q$, Ret $(g^a, a)$
- $Enc(pk, m)$: $r \leftarrow \mathbb{Z}_q$, Ret $(g^r, (pk)^r \cdot m)$
- $Dec(sk, (C_0, C_1))$: Ret $C_1/(C_0)^{sk}$

# IND-CCA security

# Agenda for this lecture

- Announcements
- Recap from last time
- Hybrid public-key encryption
- Analyzing hybrid encryption
- IND-CCA security for PKE
- Digital signatures

# Digital signatures