CSE 575: Advanced Cryptography
Fall 2024
Lecture 14

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

Announcements

- HW3 will be posted today, due 10/30

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

Hybrid public-key encryption

- RSA
- Elgamal
- Lattice-based

Factor 1000x slower,

byte-for-byte.

- 10Gb files

$\text{IND-CPA}^{0}_{\text{PKE}}$:

$(pk, sk) \leftarrow \text{PKE.Gen}$

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

Ret b

$C_0(m_0, m_1)$:

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

$\text{IND-CPA}^{1}_{\text{PKE}}$:

$(pk, sk) \leftarrow \text{PKE.Gen}$

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

Ret b

$C_1(m_0, m_1)$:

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

Hybrid PKE:

PKE to encrypt key,

SKE to encrypt msg

Best of both worlds!

HPKE: RFC 9180

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

Analyzing hybrid encryption

HPKE[PKE, SKE].Gen:

Ret PKE.Gen

HPKE[PKE, SKE].Enc(pk, m):

$k \leftarrow$ SKE.Gen

$c_0 \leftarrow$ PKE.Enc(pk, k)

$c_1 \leftarrow$ SKE.Enc(k, m)

Ret c_0, c_1

HPKE[PKE, SKE].Dec(sk, c_0, c_1):

$k =$ PKE.Dec(sk, c_0)

$m =$ SKE.Dec(k, c_1)

Ret m

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

Analyzing hybrid encryption

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

$IND\text{-}CPA^{\mathcal{A}}_{HPKE}$:

$(pk, sk) \leftarrow PKE.Gen$
$b \leftarrow \mathcal{A}^{C_b(\cdot,\cdot)}(pk)$
Ret b

$C_0(m_0, m_1)$:
$k \leftarrow SKE.Gen$
$c_0^* \leftarrow PKE.Enc(pk, k)$
$c_1^* \leftarrow SKE.Enc(k, m_0)$
Ret c_0^*, c_1^*

$H_1^{\mathcal{A}}$:

$(pk, sk) \leftarrow PKE.Gen$
$b \leftarrow \mathcal{A}^{C_b(\cdot,\cdot)}(pk)$
Ret b

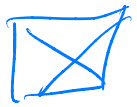
$C_0(m_0, m_1)$:
$k \leftarrow SKE.Gen$
$c_0^* \leftarrow PKE.Enc(pk, 0)$
$c_1^* \leftarrow SKE.Enc(k, m_0)$
Ret c_0^*, c_1^*

$H_2^{\mathcal{A}}$:

$(pk, sk) \leftarrow PKE.Gen$
$b \leftarrow \mathcal{A}^{C_1(\cdot,\cdot)}(pk)$
Ret b

$C_1(m_0, m_1)$:
$k \leftarrow SKE.Gen$
$c_0^* \leftarrow PKE.Enc(pk, 0)$
$c_1^* \leftarrow SKE.Enc(k, m_1)$
Ret c_0^*, c_1^*

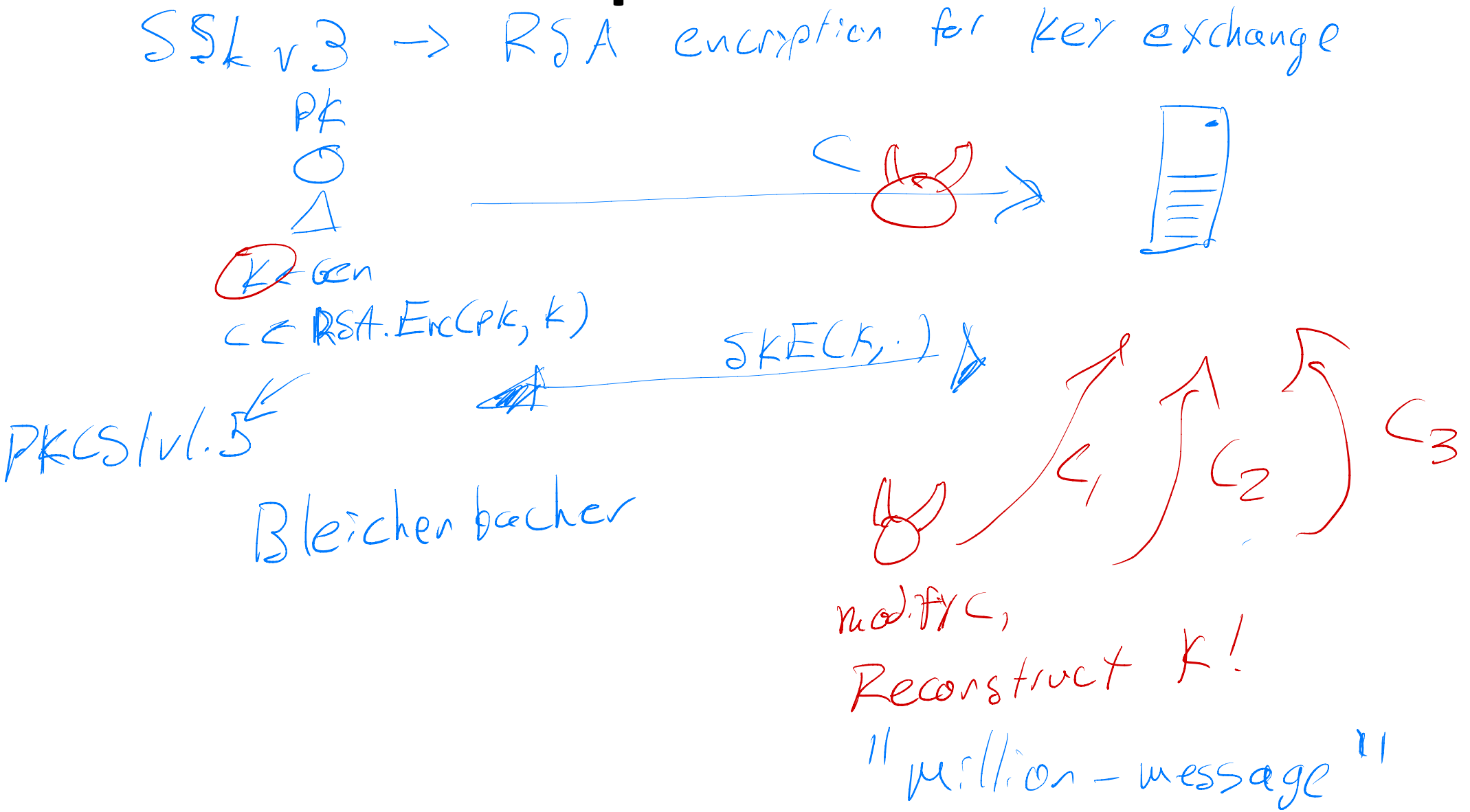
H_3: as H_2 except
$c_0^* \leftarrow PKE.Enc(pk, k)$



Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

Chosen ciphertext attacks



IND-CCA security for PKE

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

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

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

Ret b

$C_0(m_0, m_1)$:

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

Ret c^*

$Dec(c)$:

If $c \neq c^*$: Ret $PKE.Dec(sk, c)$

Ret $\perp$

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

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

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

Ret b

$C_1(m_0, m_1)$:

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

Ret c^*

$Dec(c)$:

If $c \neq c^*$: Ret $PKE.Dec(sk, c)$

Ret $\perp$

IND-CCA security for PKE

Thm: Elgamal PKE is not CCA-secure

Proof: Maul c_1^* by multiplying m^*.

Submit c_0^*, c_1^* to Dec.

Output either $m_0 m^*$ or $m_1 m^*$.

Divide out m^* to get m_0/m_1.

$\boxtimes$

$G = \langle g \rangle$ of order p

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

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

How to build IND-CCA PKE?

NIST PQC

Fujisaki - Okamoto (FO) transform

FO[PKE, SKE].Enc(pk, m):
  $r \leftarrow R$; $k \leftarrow G(r)$
  $c_0 \leftarrow PKE.Enc(pk, r ; H(r, m))$
  $c_1 \leftarrow SKE.Enc(k, m)$
  Ret c_0, c_1

FO[PKE, SKE].Dec(sk, c_0, c_1):
  $r = PKE.Dec(sk, c_0)$
  $k = G(r)$
  $m = SKE.Dec(k, c_1)$
  If $PKE.Enc(pk, r ; H(r, m)) = c_0$
    Ret m
  Ret $\perp$

Thm: Let PKE be OW-CPA and SKE be IND-CPA, and G, H are random oracles, then FO[PKE, SKE] is IND-CCA.

Agenda for this lecture

- Announcements
- Hybrid public-key encryption
- Analyzing hybrid encryption
- Chosen ciphertext attacks, IND-CCA security
- Building IND-CCA secure PKE
- Other PKE properties

(Key-)Anonymity for PKE