EECS 575: Advanced Cryptography
Fall 2021
Lecture 16

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

Announcements

- HW5 is online, due 11/8
- Exams are graded, scores online

Recap from last time

$PKE = (Gen, Enc, Dec)$

PKE is IND-CPA if

$Adv^{CPA}_{PKE}(A) =$

$|Pr[CPA^0(A)=1] - Pr[CPA^1(A)=1]| = negl(\lambda)$ $\forall$ nuPPT A

CPA^0:

$pk, sk \leftarrow Gen$

$b \leftarrow A^{C^0(\cdot,\cdot)}(pk)$

$C^0(m_0, m_1)$:

Ret $Enc_{pk}(m_0)$

CPA^1:

$pk, sk \leftarrow Gen$

$b \leftarrow A^{C^1(\cdot,\cdot)}(pk)$

$C^1(m_0, m_1)$:

Ret $Enc_{pk}(m_1)$

Recap from last time

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

* Gen: $a \leftarrow \mathbb{Z}_q$

  Return (g^a, a) $\in \mathbb{G}$

* Enc$(pk = g^a, m)$: $m \leftarrow \mathbb{G}$

  $r \leftarrow \mathbb{Z}_q$; $R = g^r$

  Ret. $(R, pk^r \cdot m)$

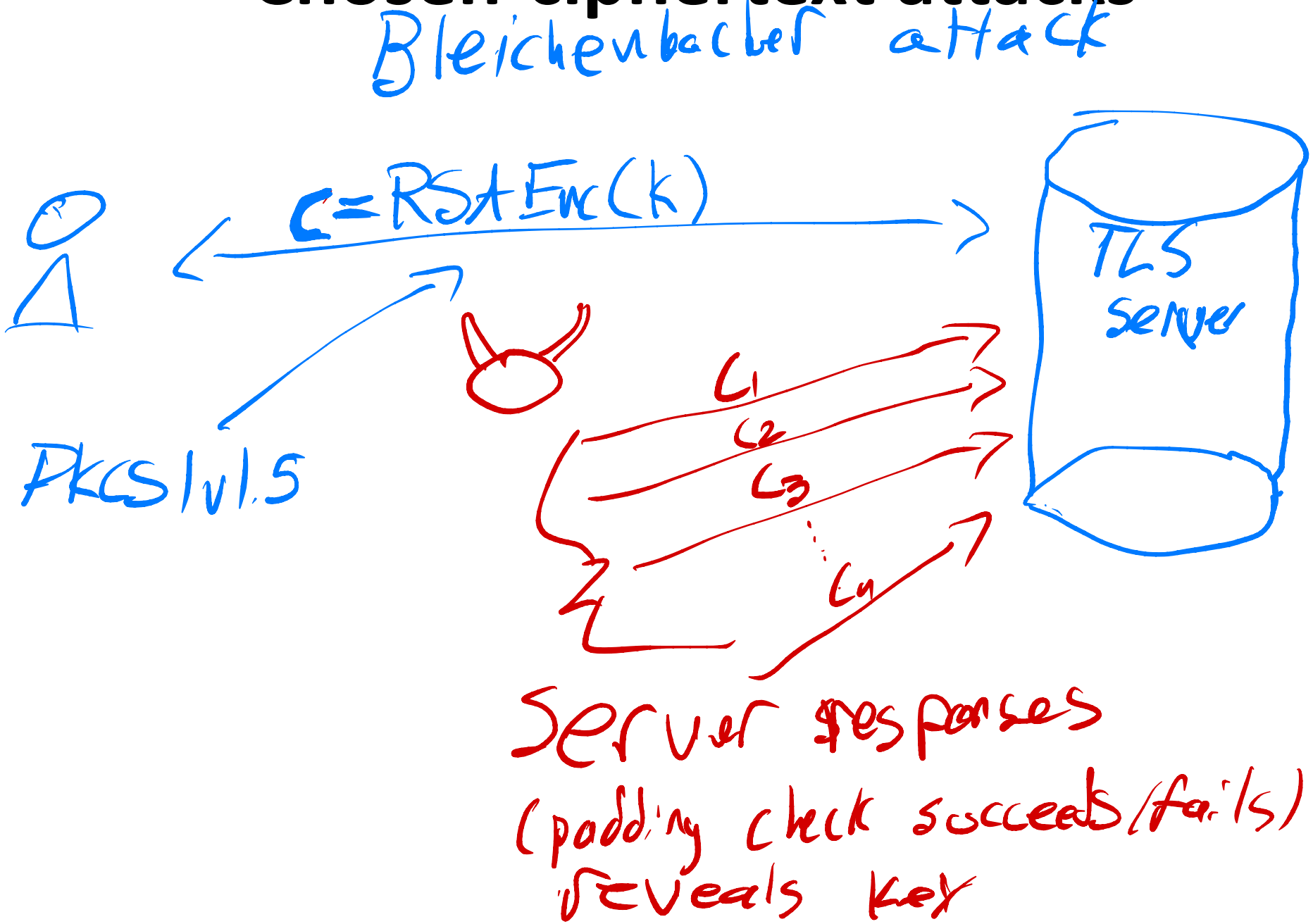
* Dec$(sk, c = (c_0, c_1))$:

  Ret c_1 / c_0^{sk}

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

Chosen-ciphertext attacks



IND-CCA

Chosen-ciphertext attacks

CCA^0:

$pk, sk \leftarrow Gen$

$b \leftarrow A^{C^0(\cdot,\cdot), Dec}(pk)$

$C^0(m_0, m_1)$:

Ret $c^* = Enc_{pk}(m_0)$

$Dec(c)$:

If $c \neq c^*$:

Ret $Dec(sk, c)$

CCA^1:

$pk, sk \leftarrow Gen$

$b \leftarrow A^{C^1(\cdot,\cdot), Dec}(pk)$

$C^1(m_0, m_1)$:

Ret $c^* = Enc_{pk}(m_1)$

$Dec(c)$:

If $c \neq c^*$:

Ret $Dec(sk, c)$

$$Adv^{PKE}_{CCA}(A) = |Pr[CCA^0(A)=1] - Pr[CCA^1(A)=1]|$$

(PKE is IND-CCA if $\cdot$ is $negl(\cdot)$ $\forall$ nuppt A.

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

ElGamal against CCA

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

* Gen: $a \leftarrow \mathbb{Z}_q$
  Return (g^a, a)
* Enc$(pk = g^a, m \in \mathbb{G})$:
  $r \leftarrow \mathbb{Z}_q$; $R = g^r$
  Ret. $(R, pk^r \cdot m)$
* Dec$(sk, c = (c_0, c_1))$:
  Ret c_1 / c_0^{sk}

$A(pk)$:

$c^* \leftarrow \bar{E}(m_0, m_1)$ ←

$(R, c') = c^*$

$D \in \mathbb{G}$; $c'' = c' \cdot D$

input c^*

$m' \leftarrow \bar{Dec}((R, c''))$ ←

If $m' = m_0 \cdot D$ Ret 0

Else 1

Queries $\bar{Dec}$ after $\bar{c}$!

Can define relaxation of CCA security that disallows $\bar{Dec}$ after $\bar{c}$.

"Lunchtime"/CCA1

Open problem: CCA1 of ElGamal is open problem!

$Adv^{PKE}_{CCA}(A) = 1$

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

Hybrid Encryption

PKE is slow practically.
Hybrid encryption does "small" PKE to encrypt key, encrypt message with SKE.

HPKE[PKE, SKE] :

PKE = ⟨PGen, PEnc, PDec⟩
SKE = ⟨SGen, SEnc, SDec⟩

* Gen: Ret PGen
* Enc(pk, m):
  K ← SGen
  C_0 ← PEnc(pk, K)
  C_1 ← SEnc(K, m)
  Ret (C_0, C_1)
* Dec(sk, $C=C_0, C_1$)):
  K ← PDec(sk, C_0)
  If K=⊥ output ⊥ ← Remove if ⊥ is not valid sky
  m ← SDec(K, C_1)
  Ret m

→ IRTF drafting new HPKE scheme, DHIES, ECIES are Hybrid encryption standards

Hybrid Encryption

Theorem: If PKE and SKE are IND-CPA$^{CCA}_{2}$ then HPKE[PKE, SKE] is IND-CPA$^{CCA}_{2}$

Proof (sketch): By reduction. Assume we have A s.t.

$$|Pr[CPA^0(A)=1] - Pr[CPA^1(A)=1]| > 1/p(n)$$

First, define G_1. Replace $PEnc(pk, k)$ with $PEnc(pk, 0)$

$CPA^0 \approx_c G_1$ by IND-CPA of PKE

Define G_2: Replace $SEnc(K, m_0)$ with $SEnc(k, m_1)$

$G_1 \approx_c G_2$ by IND-CPA of SKE

G_3: Restore $PEnc(pk, k)$ instead of $PEnc(pk, 0)$

$G_2 \approx G_3$ by IND-CPA of PKE

Hybrid Encryption

Proof sketch

Theorem: If PKE and SKE are IND-CPA^{CCA_2} then HPKE[PKE, SKE] is IND-CPA^{CCA_2}

First, define G_1. Replace PEnc(pk, k) with PEnc(pk, 0)
$CPA^0 \approx_c G_1$ by IND-CPA of PKE

Define G_2: Replace SEnc(k, m_0) with SEnc(k, m_1)
$G_1 \approx_c G_2$ by IND-CPA of SKE

G_3: Restore PEnc(pk, k) instead of PEnc(pk, 0)
$G_2 \approx G_3$ by IND-CPA of PKE

$CPA^0(t)$:

pk, sk ← PGen
$b \leftarrow A^{C^0(\cdot,\cdot)}(pk)$

$C^0(m_0, m_1)$:

k ← SGen
$c_0 \leftarrow$ PEnc(pk, k)
$c_1 \leftarrow$ SEnc(k, m_b)
Ret (c_0, c_1)

$G_1(t)$:

pk, sk ← PGen
$b \leftarrow A^{C^0(\cdot,\cdot)}(pk)$

$C^0(m_0, m_1)$:

k ← SGen
$c_0 \leftarrow$ PEnc(pk, 0)
$c_1 \leftarrow$ SEnc(k, m_b)
Ret (c_0, c_1)

To show $CPA^0 \approx_c G_1$,
reduce to IND-CPA of PKE

$B^{t, C(\cdot,\cdot)}(pk)$:

$b \leftarrow A^{\tilde{C}(\cdot,\cdot)}(pk)$
Ret b

If B's oracle is C^0, CPA^0
If C^1, CPA^1.

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

k ← SGen
$c_0^* \leftarrow C(k, 0)$
Ret c_0^*, SEnc(k, m_b)

Hybrid Encryption

Theorem: If PKE and SKE are IND-CPA$^{CCA}_2$ then HPKE[PKE, SKE] is IND-CPA^{CCA}

Proof sketch

First, define G_1. Replace PEnc(pk, k) with PEnc(pk, 0)
$CPA^0 \approx_c G_1$ by IND-CPA of PKE

Define G_2: Replace SEnc(k, m0) with SEnc(k, m1)
$G_1 \approx_c G_2$ by IND-CPA of SKE

G_3: Restore PEnc(pk, k) instead of PEnc(pk, 0)
$G_2 \approx G_3$ by IND-CPA of PKE

$CPA^0(k)$:
pk, sk ← PGen
$b \leftarrow A^{C^0(\cdot,\cdot)}(pk)$

$C^0(m_0, m_1)$:
K ← SGen
$c_0 \leftarrow$ PEnc(pk, k)
$c_1 \leftarrow$ SEnc(K, m_0)
Ret (c_0, c_1)

$G_1(k)$:
pk, sk ← PGen
$b \leftarrow A^{C(\cdot,\cdot,\cdot)}(pk)$

$C(m_0, m_1)$:
K ← SGen
$c_0 \leftarrow$ PEnc(pk, 0)
$c_1 \leftarrow$ SEnc(K, m_0)
Ret (c_0, c_1)

$G_2(k)$:
pk, sk ← DGen
$b \leftarrow A^{C(\cdot,\cdot,\cdot)}(pk)$

$C(m_0, m_1)$:
K ← SGen
$c_0 \leftarrow$ PEnc(pk, 0)
$c_1 \leftarrow$ SEnc(K, m_1)
Ret (c_0, c_1)

$G_1 \approx_c G_2$ by reduction to IND-CPA of SKE.
Use similar arg. as before
Remainder of proof is exercise

Agenda for this lecture

- Announcements
- Recap from last time
- Chosen-ciphertext attacks
- CCA insecurity of ElGamal
- Hybrid encryption
- Digital signatures

Digital Signatures