CSE 575: Advanced Cryptography
Fall 2024
Lecture 9

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

Announcements

- HW2 online, due ~~9/26~~ 9/30 11:59pm

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

SKE from a PRG

Let $G : \{0,1\}^{n/2} \to \{0,1\}^n$ be PRG

- Gen: $k \leftarrow \{0,1\}^{n/2}$
- Enc(k, m): Ret $m \oplus G(k)$
- Dec(k, c): Ret $c \oplus G(k)$

Exercise: $\exists$ SKE that is SS but not PR

Thm: If G is PRG, SKE[G] is PR

Proof: Let $m \in \{0,1\}^n$

$\{k \leftarrow Gen : Enc(k, m)\} = \{m \oplus G(k)\} = H_0$

$\{p \leftarrow U_n ; m \oplus p\} = H_1$,

$\{U_n\} = H_2$

$H_0 \approx_c H_1 \approx_s H_2$

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

IND-CPA security

$C_b(M_0, M_1)$:

Ret $Enc(K, M_b)$

SKE is IND-CPA if $\forall$ nuPPT

$\{K \leftarrow Gen : C_0(\cdot,\cdot)\} \approx_c \{K \leftarrow Gen : C_1(\cdot,\cdot)\}$

$IND\text{-}CPA0^{\mathcal{A}}_{SKE}$:

$K \leftarrow Gen$

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

Ret b

$IND\text{-}CPA1^{\mathcal{A}}_{SKE}$:

$K \leftarrow Gen$

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

Ret b

$$\left| Pr[IND\text{-}CPA0^{\mathcal{A}}_{SKE} = 1] - Pr[IND\text{-}CPA1^{\mathcal{A}}_{SKE} = 1] \right| = negl(n)$$

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

SKE from a PRF

n-bit strings

$f : \{0,1\}^n \to \{0,1\}^n$

CTR[F]:

- Gen: $k \leftarrow \{0,1\}^n$
- Enc(k, m):
  $r \leftarrow \{0,1\}^n$
  Ret $(r, F_k(r) \oplus m)$
- Dec(k, c):
  Parse c as r, c_0
  Ret $c_0 \oplus F_k(r)$

Thm: If f PRF, CTR[f] is IND-CPA.

Proof:

Replace PRF with RF, use conditioning argument to "get rid" of r collisions.

Analyzing the scheme

Lemma:

Let A, B, F be events.

If $A \wedge \neg F \iff B \wedge \neg F$

then

$|Pr[A] - Pr[B]| \leq Pr[F]$.

"identical-until-bad" lemma

Proof: Since $A \wedge \neg F \iff B \wedge \neg F$,

$Pr[A \wedge \neg F] = Pr[B \wedge \neg F]$.

Thus,

$|Pr[A] - Pr[B]| =$

$|Pr[A \wedge F] + Pr[A \wedge \neg F]$

$- Pr[B \wedge F] - Pr[B \wedge \neg F]|$

$= |Pr[A \wedge F] - Pr[B \wedge F]|$

$\leq Pr[F]$

Analyzing the scheme

$\mathrm{IND\text{-}CPA}^{\mathcal{A}}_{\mathrm{CTR}[F]}$:

$K \leftarrow \{0,1\}^n$

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

Ret b

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

$r \leftarrow \{0,1\}^n$

Ret $(r, m_0 \oplus F_K(r))$

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

$T \leftarrow [\,]$

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

Ret b

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

$r \leftarrow \{0,1\}^n$

If $T[r] = 1$

$p \leftarrow \{0,1\}^n$

set $T[r] = p$

Ret $(r, m_0 \oplus T[r])$

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

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

Ret b

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

$r \leftarrow \{0,1\}^n$

$p \leftarrow \{0,1\}^n$

Ret $(r, p \oplus m_0)$

Agenda for this lecture

- Announcements
- SKE from a PRG
- IND-CPA security
- IND-CPA secure SKE from a PRF
- Message authentication

Message authentication