CSE 575: Advanced Cryptography
Fall 2024
Lecture 12

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

Announcements

- Midterm out, due 10/11

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

SGCM scheme

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

SGCM[f].Enc((K, H), m):

$IV \leftarrow \{0,1\}^{n-1}$

$p = f_K(IV \| 10)$

$c = m \oplus p$

$t = c \cdot H \oplus f_K(IV \| 1)$

Ret IV, c, t

SGCM[f].Dec((K, H), c'):

Parse IV, c, t

$t' = c \cdot H \oplus f_K(IV \| 1)$

If $t = t'$:
  Ret $c \oplus f_K(IV \| 0)$

Ret $\perp$

Thm: If f is PRF, SGCM[f] is ROR.

Analyzing SGCM

Sketch:

1. replace PRF outputs w/ rand. bits
2. get rid of IV collisions
3. use "polynomial over $\mathbb{F}$" lemma to argue non-$\perp$ outputs D happen w/ negl. prob

Analyzing SGCM

$\mathrm{RO}\mathcal{O}^{\mathcal{A}}_{\mathrm{SGCM}[F]}$:

$K, H \leftarrow \{0,1\}^n$; $T = []$

$b \leftarrow \mathcal{A}^{\mathrm{Enc},\mathrm{Dec}}$

Ret b

Enc(m):

$IV \leftarrow \{0,1\}^{n-1}$

$P = f_K(IV\|0)$

$C = m \oplus P$

$t = C \cdot H \oplus f_K(IV\|1)$

Add $IV\|C\|t$ to T

Ret $IV\|C\|t$

Dec(IV, C, t):

If $IV\|C\|t$ in T: Ret $\perp$

$t' = C \cdot H \oplus f_K(IV\|1)$

If $t = t'$:

Ret $C \oplus F_K(IV\|0)$

Ret $\perp$

$H_0^{\mathcal{A}}$ $\mathrm{SGCM}[F]$:

$H \leftarrow \{0,1\}^n$; $T = []$

$b \leftarrow \mathcal{A}^{\mathrm{Enc},\mathrm{Dec}}$

Ret b

Enc(m):

$IV \leftarrow \{0,1\}^{n-1}$

$P = R(IV\|0)$

$C = m \oplus P$

$t = C \cdot H \oplus R(IV\|1)$

Add $IV\|C\|t$ to T

Ret $IV\|C\|t$

Dec(IV, C, t):

If $IV\|C\|t$ in T: Ret $\perp$

$t' = C \cdot H \oplus R(IV\|1)$

If $t = t'$:

Ret $C \oplus R(IV\|0)$

Ret $\perp$

$H_1^{\mathcal{A}}$ $\mathrm{SGCM}[F]$:

$H \leftarrow \{0,1\}^n$; $T = []$

$b \leftarrow \mathcal{A}^{\mathrm{Enc},\mathrm{Dec}}$

Ret b

Enc(m):

$IV \leftarrow \{0,1\}^{n-1}$

If IV already sampled:

Sample unseen IV

$P = R(IV\|0)$

$C = m \oplus P$

$t = C \cdot H \oplus R(IV\|1)$

Add $IV\|C\|t$ to T

Ret $IV\|C\|t$

Dec(IV, C, t):

If $IV\|C\|t$ in T: Ret $\perp$

$t' = C \cdot H \oplus R(IV\|1)$

If $t = t'$:

Ret $C \oplus R(IV\|0)$

Ret $\perp$

RORO $\to$ H_0 by PRF.

$H_0 \to H_1$ by bad-lemma.

$\leq \frac{q^2}{2^{n-1}}$

H_1 has non-$\perp$ Dec outputs

Case 1: IV new

$\leq \frac{q}{2^n}$

Case 2: IV old, C or t new

$C \cdot H \oplus R(IV\|1) = t$

$C \cdot H \oplus R(IV\|1) \neq t$

By S-2, $\leq 1/2^n$

$q/2^n$

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

Properties of SGCM

GCM-SIV

Nonce-reuse

IV, c_0, t_0 IV, c_1, t_1

$t_0 = c_0 H \oplus f_K(IV||1)$

$t_1 = c_1 H \oplus f_K(IV||1)$

$t_0 - t_1 = (c_0 - c_1) H$

$\hookrightarrow H = \frac{t_0 - t_1}{c_0 - c_1}$

Works for GCM $H = E_K(0)$

Properties of SGCM

Key Commitment

Should be hard to find ct, k_0, k_1 s.t.

$Dec(k_0, ct) \neq \perp$ and $Dec(k_1, ct) \neq \perp$

True for SGCM? No.

$$\begin{cases} C \cdot H_1 \oplus f_{k_1}(IV \| 1) = T \\ C \cdot H_2 \oplus f_{k_2}(IV \| 1) = T \end{cases}$$

Fix (H_1, k_1), (H_2, k_2), IV.

Compute $f_{k_1}(IV \| 1)$ and $f_{k_2}(IV \| 1)$

Solve for C, T. Then $IV \| C \| T$ dec's for both

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

Motivating PKE

PKE syntax

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

IND-CPA security for PKE

Agenda for this lecture

- Announcements
- Simplified GCM scheme + analysis
- Properties of SGCM
- Public-key encryption
- IND-CPA for PKE
- Group theory background and assumptions

Group theory background