EECS 575: Advanced Cryptography
Fall 2021
Lecture 2

Test of markups

Paul Grubbs

paulgrub@umich.edu

Beyster 4709

Agenda for this lecture

- Announcements
- Information-theoretic security and its limitations
- Roadmap to computational security

Agenda for this lecture

- Announcements
- Information-theoretic security and its limitations
- Roadmap to computational security

Announcements

- Homework 1 will be released today, due next Wednesday.
  - It will be short
- tentative homework schedule:
  - HW1: 9/1-9/8
  - HW2: 9/6-9/20
  - HW3: 9/20-10/1
  - HW4: 10/11-10/25
  - HW5: 10/25-11/8
  - HW6: 11/8-11/22
- Put your topic suggestions on Piazza!
- Lecture recordings should be visible on Canvas

Anthony OH:
9am - 10am Tues
2pm - 3pm Weds

Agenda for this lecture

- Announcements
- Information-theoretic security and its limitations
- Roadmap to computational security

Recap from last time

Symmetric-key encryption

- Gen takes no inputs outputs $k \in \mathcal{K}$
- $Enc(k, m)$: key $k \in \mathcal{K}$, message $m \in \mathcal{M}$ outputs ciphertext $c \in \mathcal{C}$
- $Dec(k, c)$: inputs k, c output m

$\forall m, k, c$,

$$Dec(k, Enc(k, m)) = m$$

Recap from last time

Definition 2.1 (Shannon secrecy)**.** A symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *Shannon secret with respect to a probability distribution* D over $\mathcal{M}$ if for all $\bar{m} \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{m \leftarrow D,\, k \leftarrow \mathsf{Gen}}[m = \bar{m} \mid \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow D}[m = \bar{m}].$$

The scheme is *Shannon secret* if it is Shannon secret with respect to every distribution D over $\mathcal{M}$.

$$\Pr_{m,k}[m = \bar{m} \mid Enc_k(m) = \bar{c}] = \frac{\Pr_{m,k}[m = \bar{m} \wedge Enc_k(m) = \bar{c}]}{\Pr_{m,k}[Enc_k(m) = \bar{c}]}$$

$$= \frac{\Pr_{\bar{m}}[m = \bar{m}] \Pr_{k}[Enc_k(\bar{m}) = \bar{c}]}{\Pr_{m,k}[Enc_k(m) = \bar{c}]}$$

$$\Pr_{k}[Enc_k(\bar{m}) = \bar{c}] = \Pr_{k,m}[Enc_k(m) = \bar{c}]$$

Perfect Secrecy

Definition 2.2 (Perfect secrecy)**.** A symmetric-key encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ is *perfectly secret* if for all $m_0, m_1 \in \mathcal{M}$ and all $\bar{c} \in \mathcal{C}$,

$$\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_0) = \bar{c}] = \Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m_1) = \bar{c}].$$

Shannon secrecy $\Leftrightarrow$ Perfect secrecy

The One-Time Pad

Let $n > 1$ $\quad \mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$

- Gen: outputs $k \leftarrow \{0,1\}^n$ (unif. random)
- $\mathrm{Enc}(k, m)$: output $k \oplus m$
- $\mathrm{Dec}(k, c)$: output $k \oplus c$

Correctness:

$$\mathrm{Dec}(k, \mathrm{Enc}(k, m)) = \mathrm{Dec}(k, k \oplus m)$$
$$= k \oplus (k \oplus m)$$
$$= m$$

Perfect Secrecy of the One-Time Pad

Theorem 2.4. *The one-time pad is a perfectly secret symmetric-key encryption scheme.*

Proof:

$(\bar{m}, \bar{c})$

$$\Pr_K[Enc_K(\bar{m}) = \bar{c}]$$

$$= \Pr_K[K \oplus \bar{m} = \bar{c}] \quad \text{Fixed}$$

$$= \Pr_K[K = \bar{m} \oplus \bar{c}]$$

$$= \frac{1}{2^n}$$

$\forall m_0, m_1, \bar{c}$

$$\Pr_K[Enc_K(m_0) = \bar{c}] = \Pr_K[Enc_K(m_1) = \bar{c}]$$

$$\Pr_K[K = m_0 \oplus \bar{c}] = \Pr_K[K = m_1 \oplus \bar{c}]$$

as desired ☒

Limitations of Shannon Secrecy

- If adv. secs Pad, they can decrypt
  - use the key twice, get $m_0 \oplus m_1$
  - key is as big as the message
- $\Pr[M = \bar{m} \mid Enc_K(M) = \bar{c}]$

$= \Pr[M = \bar{m}]$ $= \begin{cases} 1 & \text{for } m^* \\ 0 & \text{otherwise} \end{cases}$

- Deterministic: Equal plaintexts $\Rightarrow$ equal ciphertexts

Limitations of Shannon Secrecy

Thm: If (Gen, Enc, Dec) is Shannon secret,

$$|\mathcal{K}| \geq |\mathcal{M}|$$

Proof: SKE (Gen, Enc, Dec) has $|\mathcal{K}| < |\mathcal{M}|$.

Then SKE is not Shannon secret.

$\mathcal{D}$ is uniform over $\mathcal{M}$

K is arbitrary

$\bar{c}$ any support of

$\Pr_{k,m}[m = \bar{m} \mid Enc_k(m) = \bar{c}]$

$= \Pr[m = \bar{m}]$ if dists D over $\mathcal{M}$

$\mathcal{D} = \{Dec_k(\bar{c}) : k \in \mathcal{K}\}$

$|\mathcal{D}| \leq |\mathcal{K}| < |\mathcal{M}| \Rightarrow \exists\, m^* \in \mathcal{M} \setminus \mathcal{D}$ $\Pr_{k,m}[Enc_k(m) = \bar{c}]$

$0 = \Pr_{k,m}[m = m^* \mid Enc_k(m) = \bar{c}] \neq \Pr_{m}[m = m^*] = 1/|\mathcal{M}| > 0$

Agenda for this lecture

- Announcements
- Information-theoretic security and its limitations
- Roadmap to computational security

Computational Security

- Attack from before: enumerate all keys
  what if 2^{1000} keys
- Attacks might not be feasible for resource-bounded attackers
  - → # modelling bounded computation
    - # Hard problems for bounded computation
      - # Define security? Prove security

The Computational Model

Adversaries are algorithms (Turing machine)
"Basic" operations (add, multiply, access memory) take

- Exact set of basic ops is unimportant
  $T(n)$  $dT(n)^c$ d, c constants
  different ops

Two important things:
1. Randomness TM has infinite read-only tape of random bits (can only see poly-many bits)
   $t(x;r)$ ← defines a distrib. over A's output

The Computational Model

2. Non-uniformity (advice)

Algorithms get a string of input-length-dependent advice

L is non-uf. if $\exists$

$w_1, w_2 \ldots w_{|x|} \ldots \in \{0,1\}^*$

on input x, A gets $w_{|x|}$ as advice $n = |x|$

assume wlog $|w_{|x|}|$ is $O(n^c)$ for const $c > 0$

Asymptotics

$T(n)$ runtime of A on input length n

security parameter "amount of security"

$T(n)$ is polynomial if $T(n) = O(n^c)$

$T(n)$ is poly(n) for fixed const c

Function $V(n)$ is negligible ($V(n) = \text{negl}(n)$)

if $V(n) = o(n^{-c})$ for every const c

(little-o)

Negligible probability => "never" happening

Asymptotics

Is the product of a negligible and non-negligible function always negligible, always non-negligible, or neither?

One-Way Functions

Candidate One-Way Functions

Subset-sum

Candidate One-Way Functions

Multiplication

Questions to think about

If we replaced XOR with AND in the one-time pad, would it still be a valid encryption scheme? Would it be perfectly secret?

Can you think of some other ways cryptography is related to power? Do you agree that cryptography is *inherently* political?

Can any function be *unconditionally* one-way – i.e. the inverter I has advantage 0?

Let f be a one-way function. Is the function $g(x) = f(x)||0$ necessarily one-way?