

8/25 (11)

Discrete Math Seminar

ORGANIZER: Christine Kelley
TUESDAYS: 2:00-2:50 PM

Designing hash functions from graphs.

4 main Cryptographic Roles:

- 1) Confidentiality
- keep information from all but those authorized.
- Hash functions { 2) Data integrity
- Detect unauthorized alterations of message.
- 3) Authentication
- 4) Non-repudiation
- preventing parties from denying previous actions.

Def: A hash function h is a function satisfying:

- 1) Compression: $h: \Sigma^* \rightarrow \Sigma^{\ell-n}$
- 2) Easy to do!

Typical Use: Integrity. x is sent/stored at time T_1 ,
 $h(x)$ is computed, protected.

Let x' be msg at time T_2 .

if $h(x') = h(x)$, assume no alterations.

Problem: h is many-to-one.
Lots of "collisions"

Want collisions to be infeasible to find.

Additional Properties:

x, x' inputs, y, y' outputs

1) Preimage Resistance (PR)

Given outputs y , infeasible to find x
w/ $h(x) = y$.

2) Second Preimage Resistance (2PR)

Given x , infeasible to find
 $x' \neq x$ w/ $h(x) = h(x')$.

3) Collision Resistance (CR)

Infeasible to find any $x \neq x'$ s.t.
 $h(x) = h(x')$.

Open Talk Topic: Complexity of these attacks.

Use Cayley Graphs for hash functions.

Want to design $h: \Sigma^* \rightarrow \Sigma^n$

w/ Collision Resistance

Want: Small modifications in input text are always detected.

Setup: Choose a finite group G and gen set S s.t.
 $|S| = |\Sigma|$ and $f: \Sigma \rightarrow S$ bijection.

Compute $h(x)$:

input $x = x_1 x_2 \dots x_k$,

$h(x) = f(x_1) f(x_2) \dots f(x_k) =$ group product.

$$n = \log_{|S|} |G|$$

Graphically: Construct Cayley graph $\mathcal{G} = \mathcal{G}(G, S)$

(One vertex for each $g \in G$, directed edge

$v \xrightarrow{s_i} w$ if $w = v s_i$ for $s_i \in S$.)

Input text: Starting at e , walk along path given by x .

To prevent collisions, want large directed girth.

Prop: If a substring of k consecutive symbols is replaced by a substring of k' consecutive symbols, at least one of these has length $\geq \delta =$ dir. girth of G .

$$\max\{k, k'\} \geq \delta$$

Want to maximize δ .
Want to lower the diameter. } in competition!
Also: good expansion!

- Papers:
- LPS expander graphs '99-'00.
 - Zemor '93-'95ish
 - Zemor & Tillich (SL)