Freenet and Friend-to-Friend Routing

Alex Vondrak

ajvondrak@csupomona.edu

May 18, 2011

Foreword

- Not my usual fare. . .
  - Adapted from presentation for CS 565 ($\approx$ CS 380 with presentations)
  - The Good News: I'm not an expert
  - The Bad News: I'm not an expert
- Reviews were positive, despite talk being crammed into 20 minutes
- Hypothesis:

Foreword

- Not my usual fare...
  - Adapted from presentation for CS 565 ($\approx$ CS 380 with presentations)
  - The Good News: I'm not an expert
  - The Bad News: I'm not an expert
- Reviews were positive, despite talk being crammed into 20 minutes
- Hypothesis:

$$\text{talk} + \text{pretty pictures} - \text{math} = \text{WIN}$$

Peer-to-Peer Networks

In case you've been living under a rock for the past 10 years. . .

Definition (P2P Computing)

- Distributed application architecture
- Resources pooled together for "greater good"
- Peers share workload (more-or-less) equally across a network

Examples

That's easy!

- BitTorrent
- Napster
- Kazaa
- Limewire
- . . .

Peer-to-Peer Applications

P2P computing is about more than illegal file-sharing:

“Sky Peer-to-Peer”

- Internet telephony
- Built by some of the original Kazaa authors
- Closed-source; protocol specs unavailable

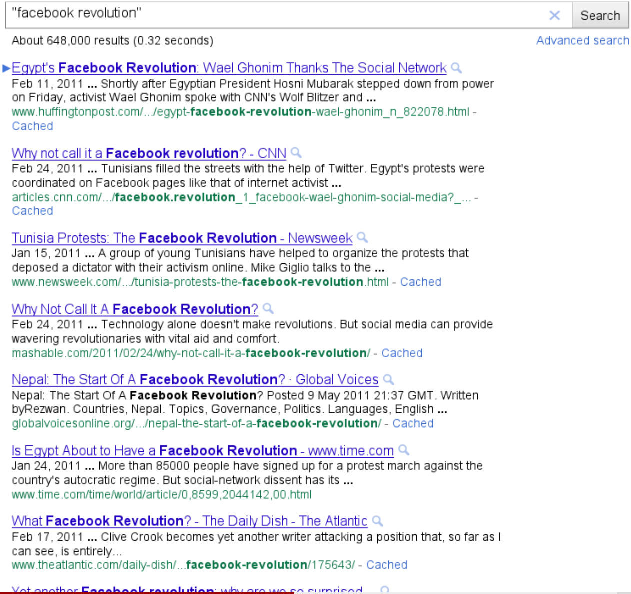
Bitcoin

- Decentralized digital currency
- Records transactions in a P2P database
- Uses cryptography to protect against fraud

Freenet

- Censorship-resistant data storage
- Distributed, decentralized architecture
- Aims to protect free speech

The Internet Is Too Big To Be Controlled



"facebook revolution"

About 648,000 results (0.32 seconds)

Egypt's **Facebook Revolution**: Wael Ghonim Thanks The Social Network
Feb 11, 2011 **...** Shortly after Egyptian President Hosni Mubarak stepped down from power on Friday, activist Wael Ghonim spoke with CNN's Wolf Blitzer and **...**
www.huffingtonpost.com/.../egypt-**facebook-revolution**-wael-ghonim_n_822078.html - Cached

Why not call it a **Facebook revolution**? - CNN
Feb 24, 2011 **...** Tunisians filled the streets with the help of Twitter. Egypt's protests were coordinated on Facebook pages like that of internet activist **...**
articles.cnn.com/.../**facebook.revolution**_1_facebook-wael-ghonim-social-media?_... - Cached

Tunisia Protests: The **Facebook Revolution** - Newsweek
Jan 15, 2011 **...** A group of young Tunisians have helped to organize the protests that deposed a dictator with their activism online. Mike Giglio talks to the **...**
www.newsweek.com/.../tunisia-protests-the-**facebook-revolution**.html - Cached

Why Not Call It A **Facebook Revolution**?
Feb 24, 2011 **...** Technology alone doesn't make revolutions. But social media can provide wavering revolutionaries with vital aid and comfort.
mashable.com/2011/02/24/why-not-call-it-a-**facebook-revolution**/ - Cached

Nepal: The Start Of A **Facebook Revolution**? · Global Voices
Nepal: The Start Of A **Facebook Revolution**? Posted 9 May 2011 21:37 GMT. Written byRezwan. Countries, Nepal. Topics, Governance, Politics. Languages, English **...**
globalvoicesonline.org/.../nepal-the-start-of-a-**facebook-revolution**/ - Cached

Is Egypt About to Have a **Facebook Revolution** - www.time.com
Jan 24, 2011 **...** More than 85000 people have signed up for a protest march against the country's autocratic regime. But social-network dissent has its **...**
www.time.com/time/world/article/0,8599,2044142,00.html

What **Facebook Revolution**? - The Daily Dish - The Atlantic
Feb 17, 2011 **...** Clive Crook becomes yet another writer attacking a position that, so far as I can see, is entirely...
www.theatlantic.com/daily-dish/...**facebook-revolution**/175643/ - Cached

Yet another **Facebook revolution**: why are we so surprised ...

“The Internet Is Too Big To Be Controlled”

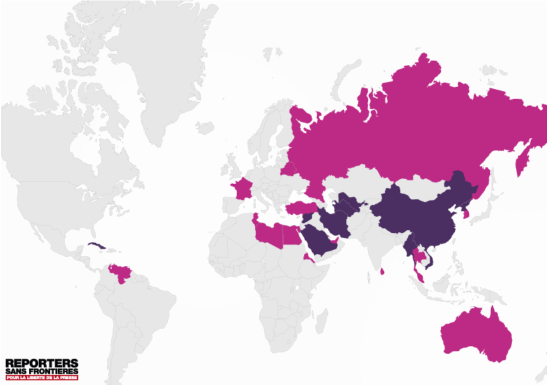
- China
  - The Great Firewall of China employs IP, URL, DNS, and packet filtering
  - “Tiananmen”, “Dalai Lama”, “democracy”, “human rights”, . . .
  - Authorities monitor blogging platforms, remove posts

- Iran
  - Hossein Derakhshan: blogger sentenced to 19.5 years after being held without charge since 2008
  - Saeed Malekpour & Vahid Asghari: website admins sentenced to death for “agitating against the regime” and “insulting the sanctity of Islam”

- Australia
  - Maintains secret blacklist of banned sites
  - WikiLeaks (2009) reports banned YouTube videos, poker sites, . . .

Internet Censorship World Map

- Burma, China, Cuba, Iran, North Korea, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, Vietnam
- Australia, Bahrain, Belarus, Egypt, Eritrea, France, Libya, Malaysia, Russia, South Korea, Sri Lanka, Thailand, Tunisia, Turkey, United Arab Emirates, Venezuela



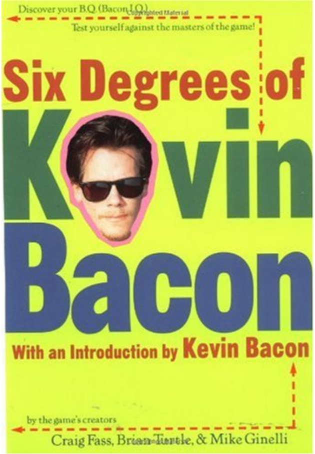
Censorship Resistance

How do we build a censorship-resistant network?

- Data must be available to everyone
- Content must be hard to get rid of
- We must protect the anonymity of...
  - those who publish content
  - those who access content
- Should protect from outsiders...
- But we also need to protect from others in the network

(Most of these topics are beyond our scope)

Friend-to-Friend Networks


Discover your B.Q. (Bacon I.Q.)
Copyrighted Material
Test yourself against the masters of the game!
Six Degrees of Kevin Bacon
With an Introduction by Kevin Bacon
by the game's creators
Craig Fass, Brian Turtle, & Mike Ginelli

Freenet

- Initially released in 2000
- In latest network architecture, you only connect to trusted peers
- Routing through the network means finding paths between friends
- This works since humans tend to form a small world network
    - Many "short" connections
    - Few "long" connections
    - Milgram's small-world experiment

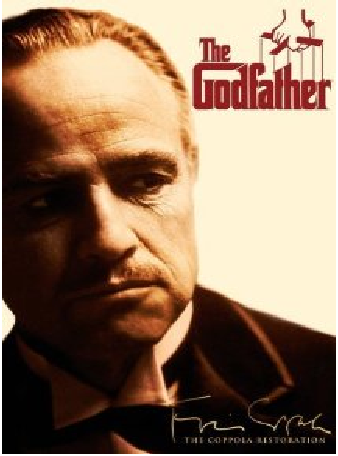
Friend-to-Friend Networks In Pop Culture

Charlie Chaplin

Friend-to-Friend Networks In Pop Culture

Charlie Chaplin

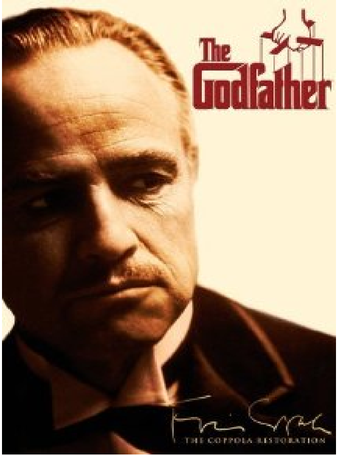
Marlon Brando



A Countess from Hong Kong (1967)

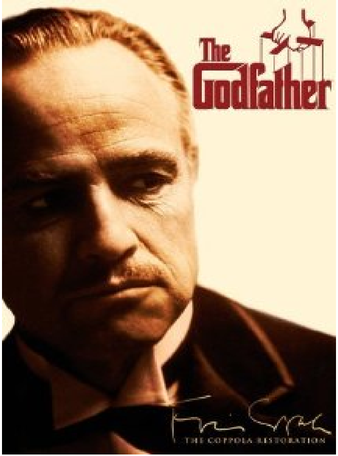
Friend-to-Friend Networks In Pop Culture

Marlon Brando



Friend-to-Friend Networks In Pop Culture

Marlon Brando



Laurence Fishburne

Apocalypse Now (1979)

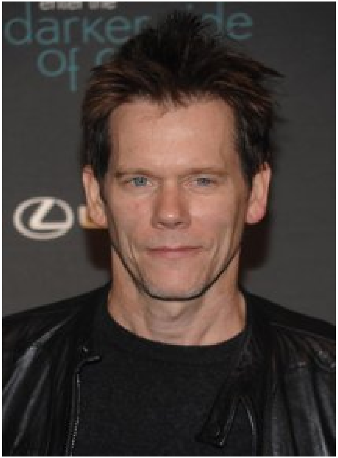
Friend-to-Friend Networks In Pop Culture

Laurence Fishburne

Friend-to-Friend Networks In Pop Culture

Laurence Fishburne

Kevin Bacon



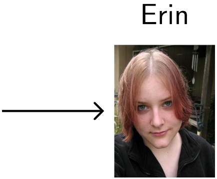
Mystic River (2003)

Routing

Me

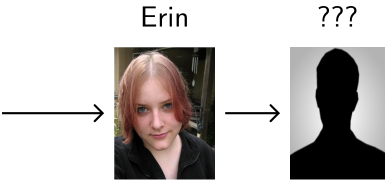
President Obama

Routing



Erin

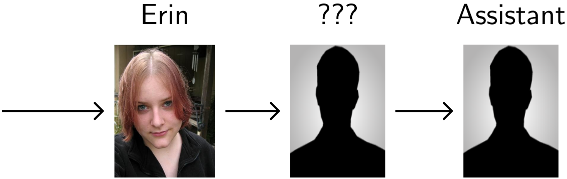
Routing



Erin

???

Routing

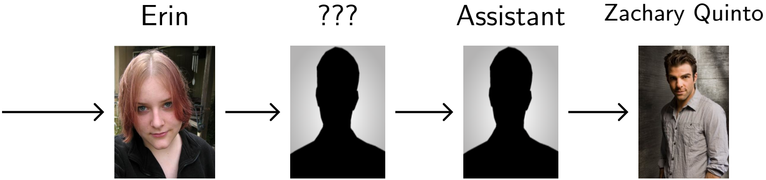


Erin

???

Assistant

Routing



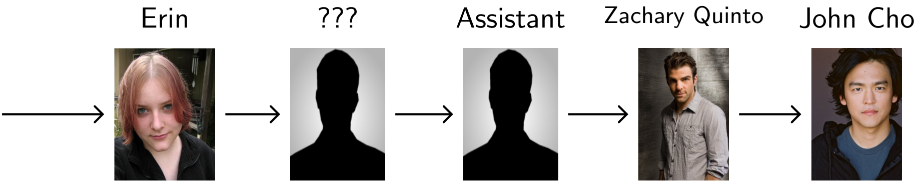
Erin

???

Assistant

Zachary Quinto

Routing



Erin

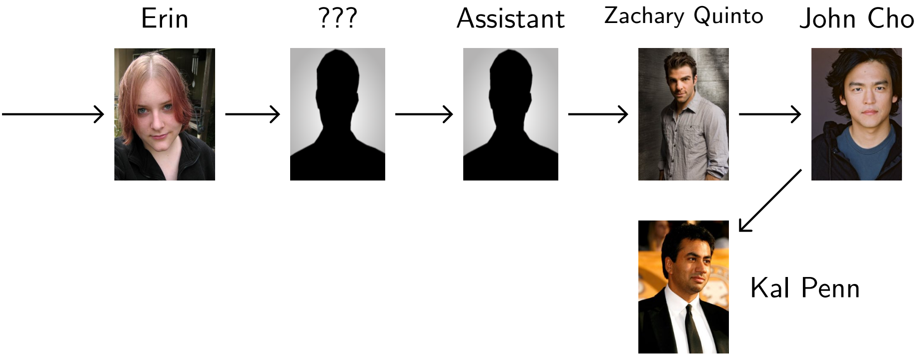
???

Assistant

Zachary Quinto

John Cho

Routing



Erin

???

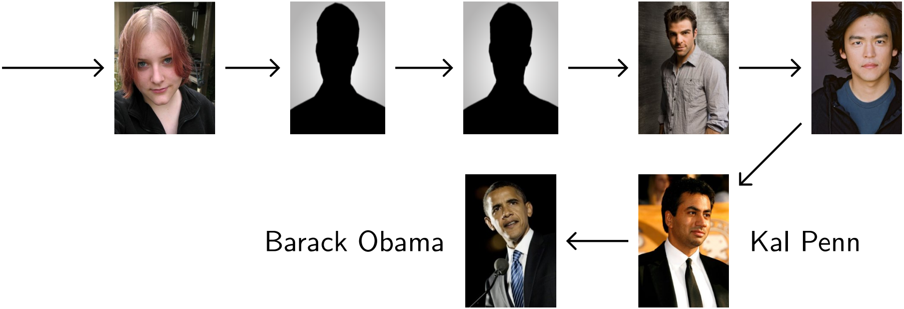
Assistant

Zachary Quinto

John Cho

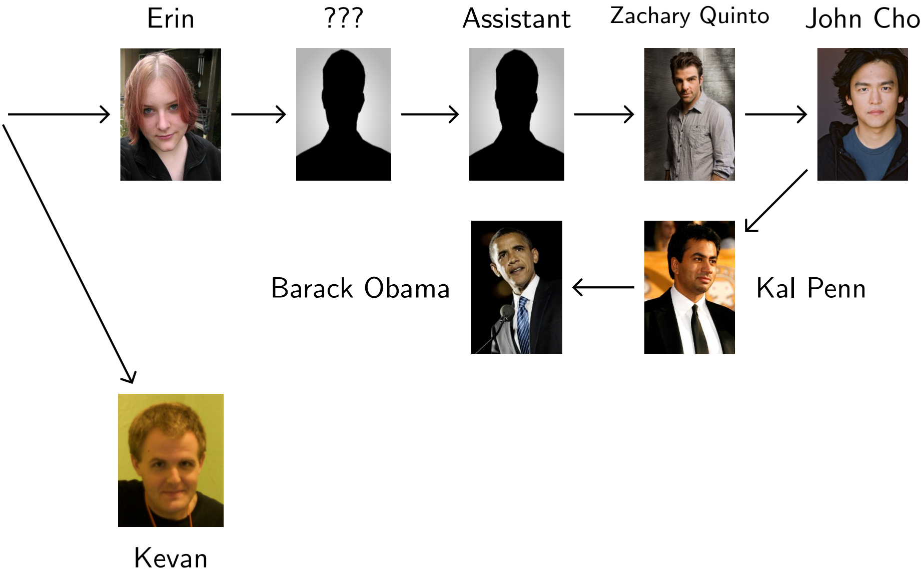
Kal Penn

Routing



Erin → ??? → Assistant → Zachary Quinto → John Cho → Kal Penn → Barack Obama

Routing



Erin

???

Assistant

Zachary Quinto

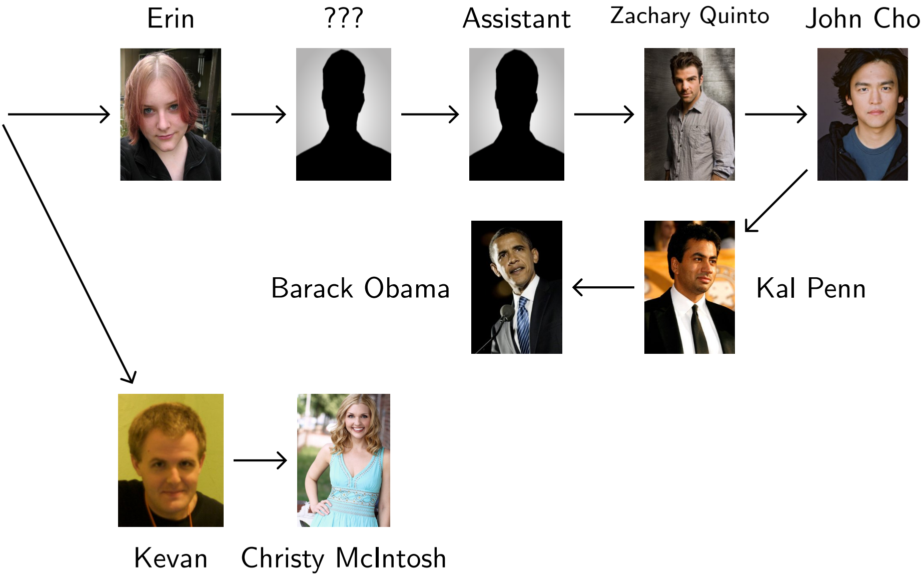
John Cho

Kal Penn

Barack Obama

Kevan

Routing



Erin

???

Assistant

Zachary Quinto

John Cho

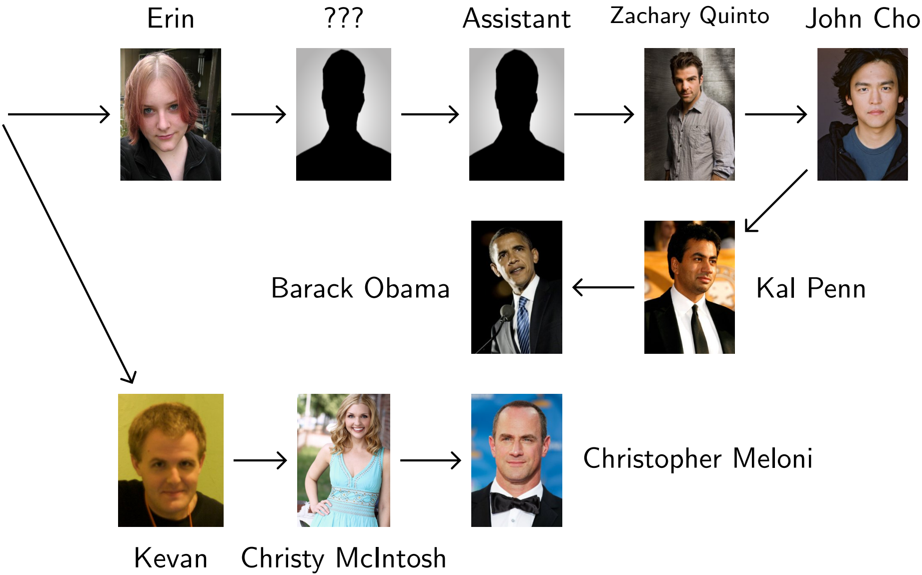
Kal Penn

Barack Obama

Kevan

Christy McIntosh

Routing



Erin

???

Assistant

Zachary Quinto

John Cho

Kal Penn

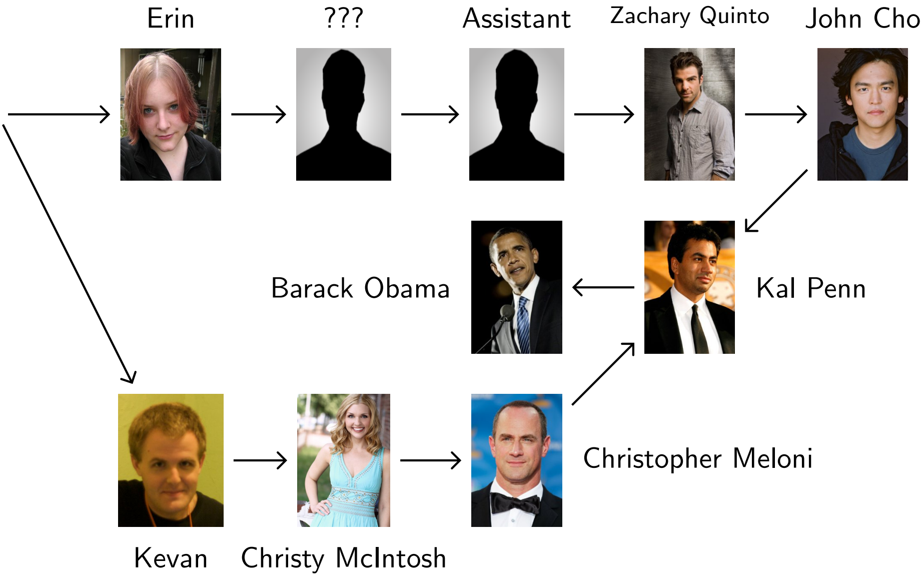
Barack Obama

Kevan

Christy McIntosh

Christopher Meloni

Routing



Erin

???

Assistant

Zachary Quinto

John Cho

Barack Obama

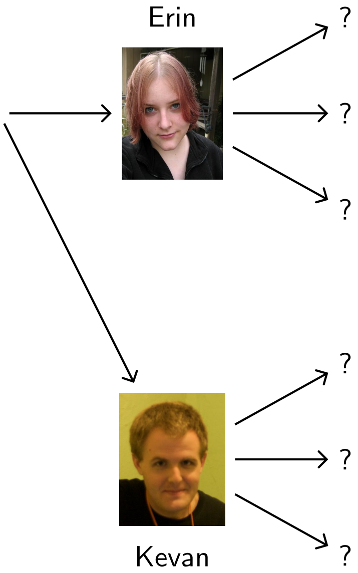
Kal Penn

Christopher Meloni

Kevan

Christy McIntosh

Routing



Erin

? ? ?

?

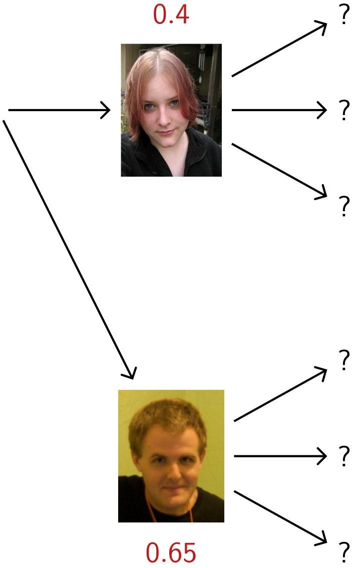
? ?

Kevan

Things to notice:

- Local
  - Decentralized
  - Only send to / receive from friends
  - Doesn't guarantee a fixed path
- Greedy algorithm
  - Everyone chooses best neighbor
  - . . . But who is "best"?
- "Closeness"

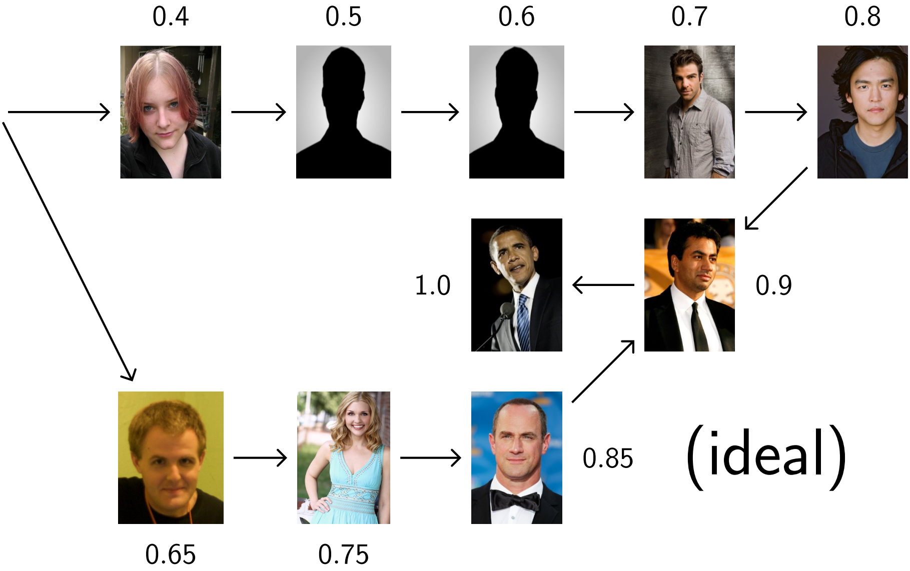
IDs



Idea:

- Assign IDs in range $[0, 1]$
- Let's say my ID is 0.3
- Let's say Obama has ID 1.0
- Choose neighbor with ID closest to destination

IDs

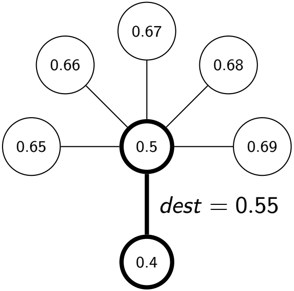


(ideal)

IDs

Problems:

- How do we deal with dead ends? Loops? Overly long paths?

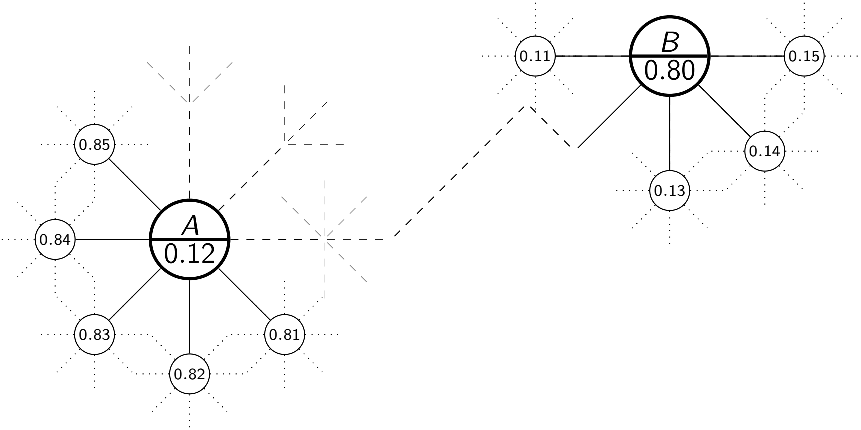


- How do we assign IDs optimally?
  - Small world: your friends have IDs close to yours
  - Kleinberg model guarantees $O(\log^2 n)$ greedy routing
- How do we assign IDs at all?
  - No one should know the entire network!

Swapping

Idea:

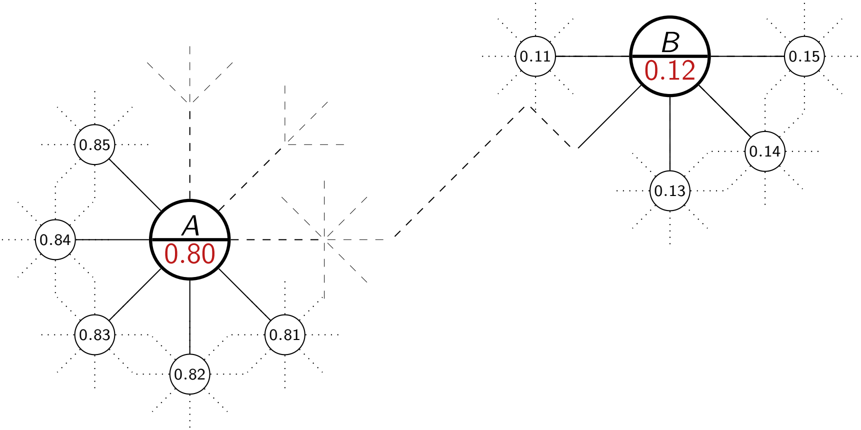
- When a node joins the network, assign a random ID
- Use the friend-of-friends connections to reverse engineer a better ID
- Instance of Metropolis-Hastings Algorithm (like simulated annealing)



Swapping

Idea:

- When a node joins the network, assign a random ID
- Use the friend-of-friends connections to reverse engineer a better ID
- Instance of Metropolis-Hastings Algorithm (like simulated annealing)

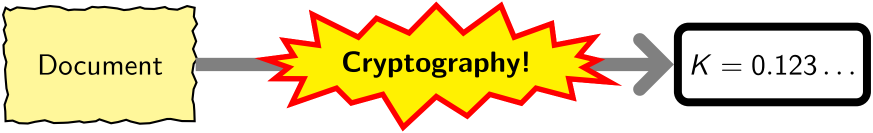


Data

Idea:

- Associate data with an ID (like the nodes)
- Use routing technique to store data along path
- Same idea applies to retrieving data

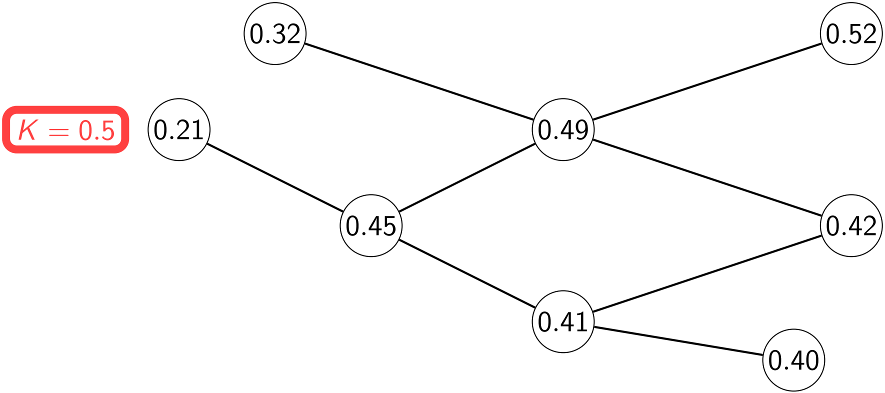
First, we get an ID from the data; the process goes roughly like...



Storing Data

Short-term cache: populated whenever we route data

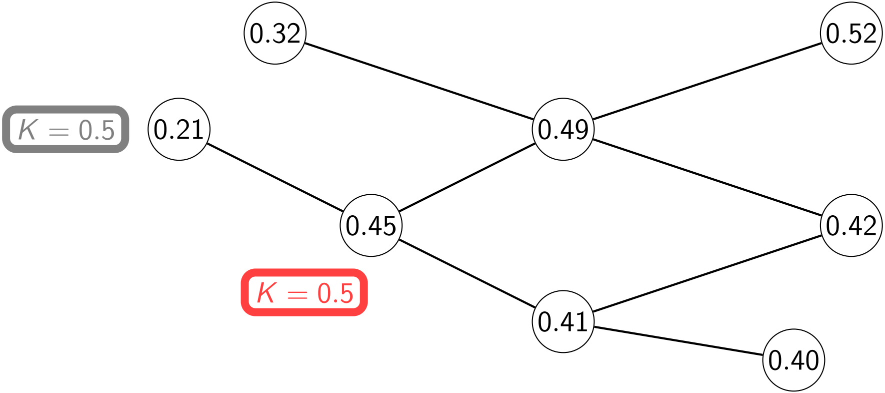
Long-term cache: populated if ID is closer than all neighbors'



Storing Data

Short-term cache: populated whenever we route data

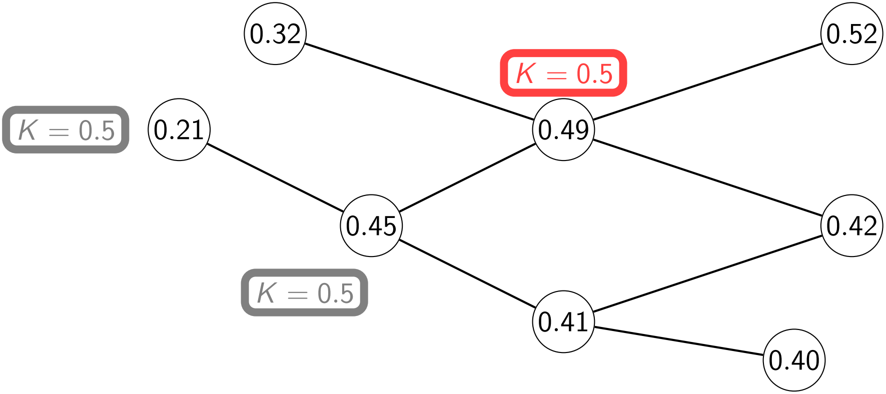
Long-term cache: populated if ID is closer than all neighbors'



Storing Data

Short-term cache: populated whenever we route data

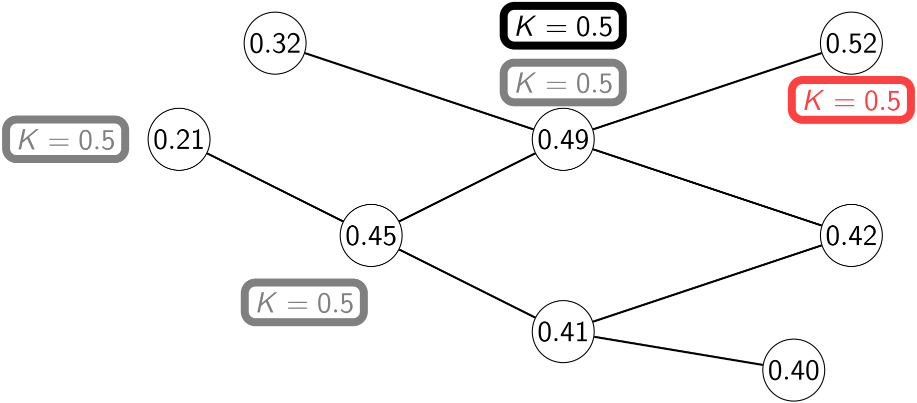
Long-term cache: populated if ID is closer than all neighbors'



Storing Data

Short-term cache: populated whenever we route data

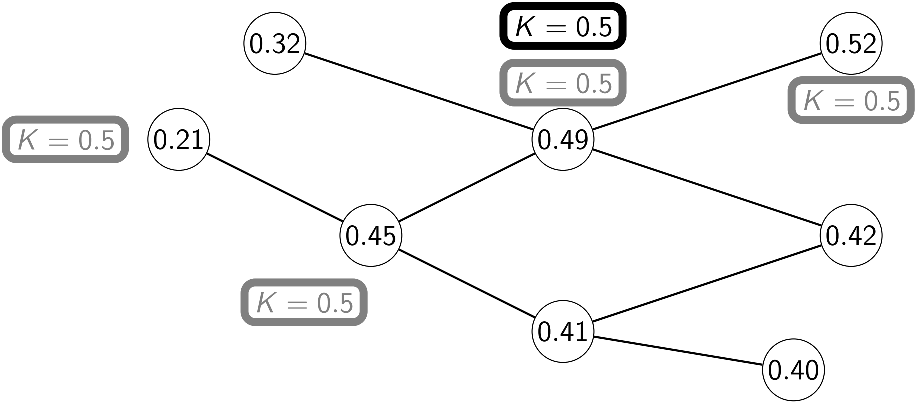
Long-term cache: populated if ID is closer than all neighbors'



Storing Data

Short-term cache: populated whenever we route data

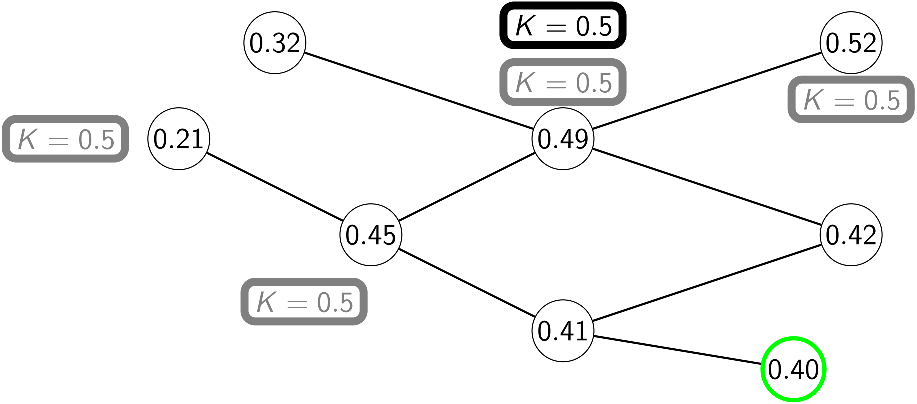
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

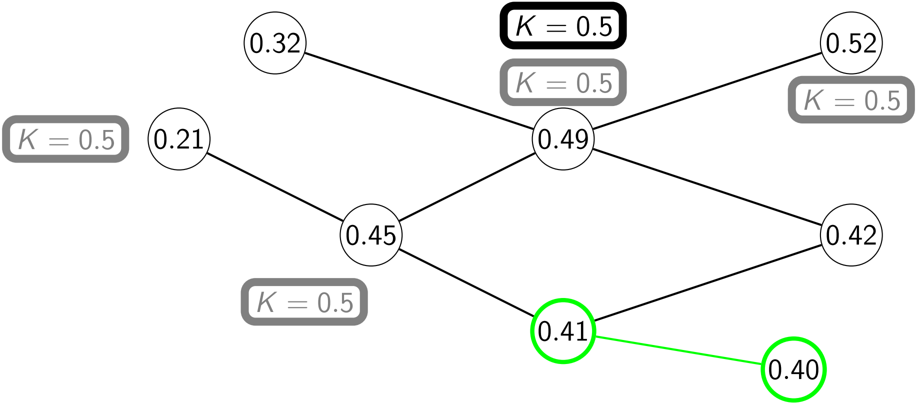
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

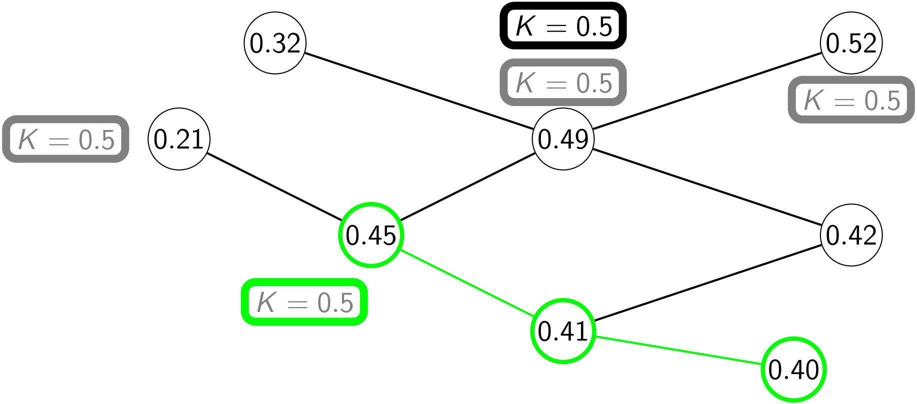
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

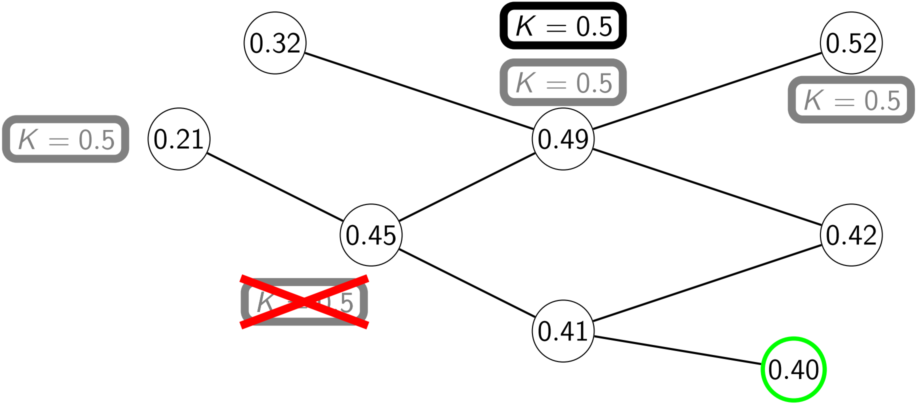
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

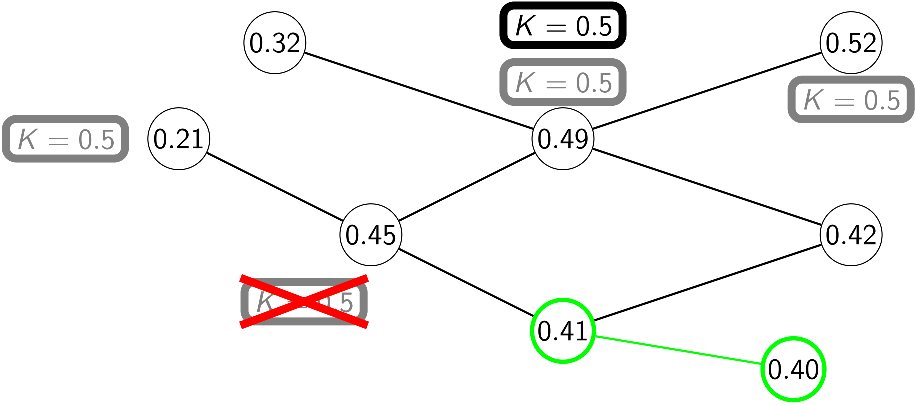
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

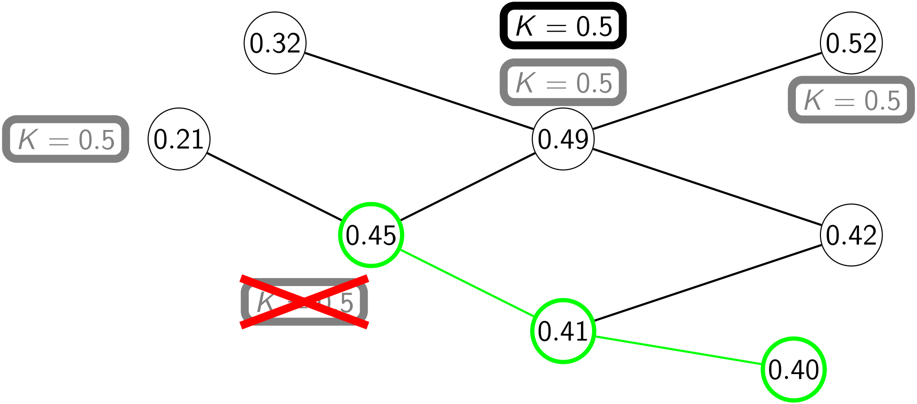
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

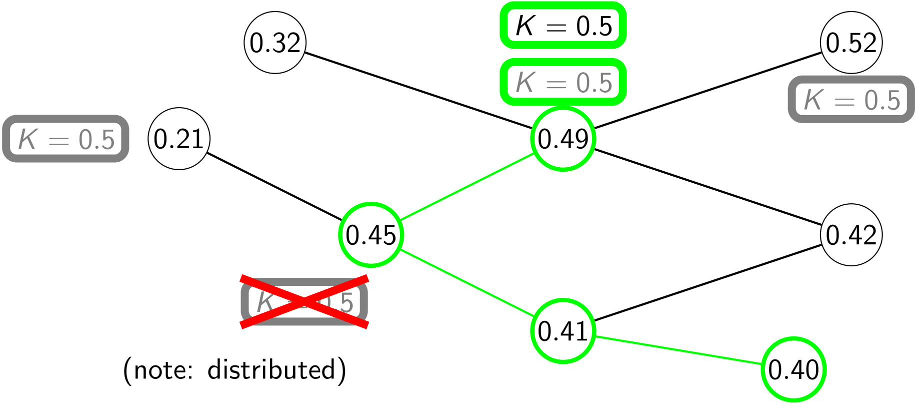
Long-term cache: populated if ID is closer than all neighbors'



Retrieving Data

Short-term cache: populated whenever we route data

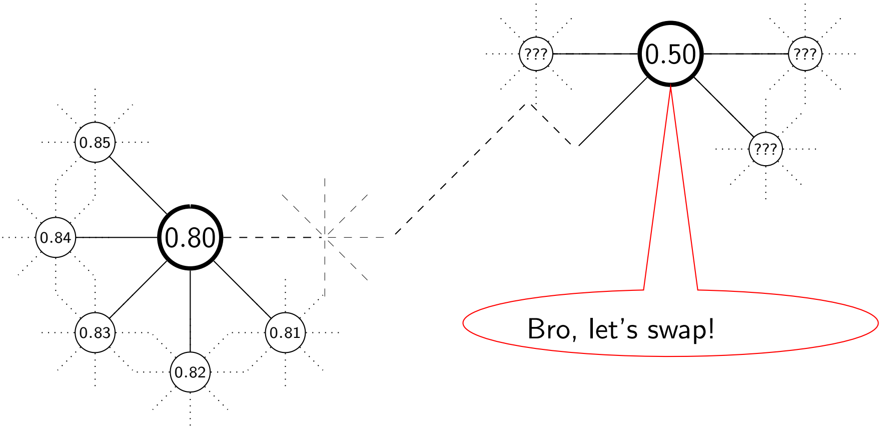
Long-term cache: populated if ID is closer than all neighbors'



(note: distributed)

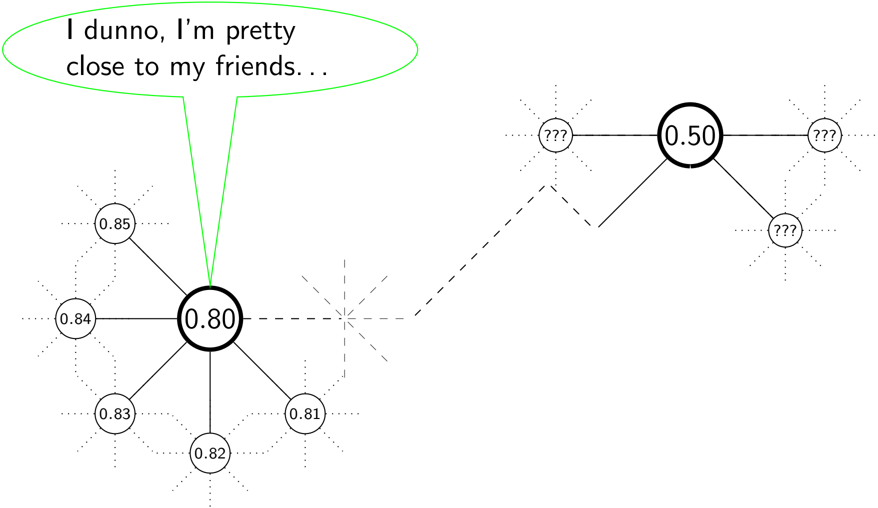
Problems

- Swap requests can't be authenticated



Problems

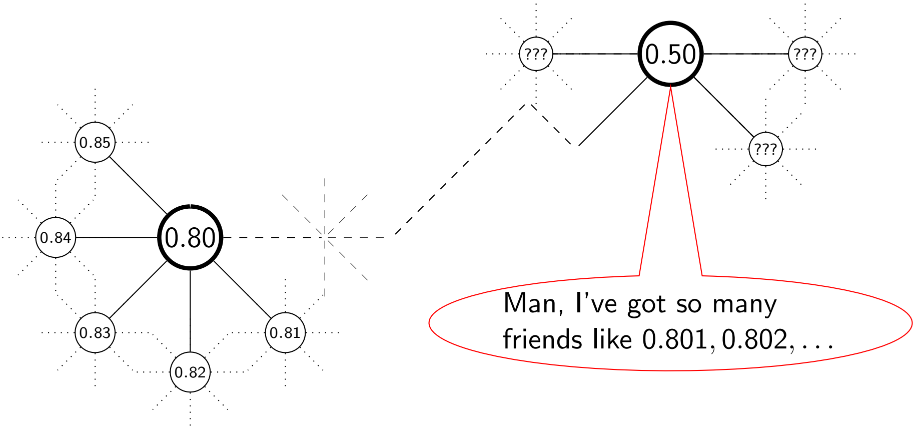
- Swap requests can't be authenticated



I dunno, I'm pretty
close to my friends. . .

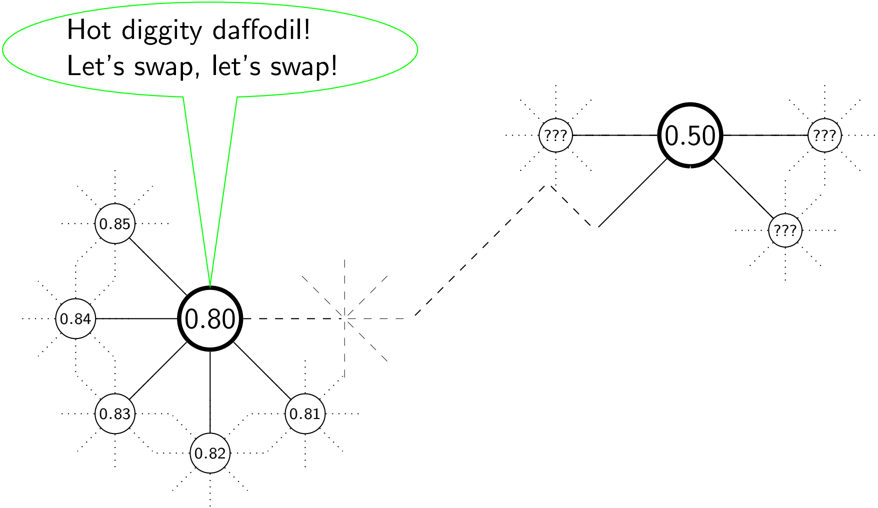
Problems

- Swap requests can't be authenticated



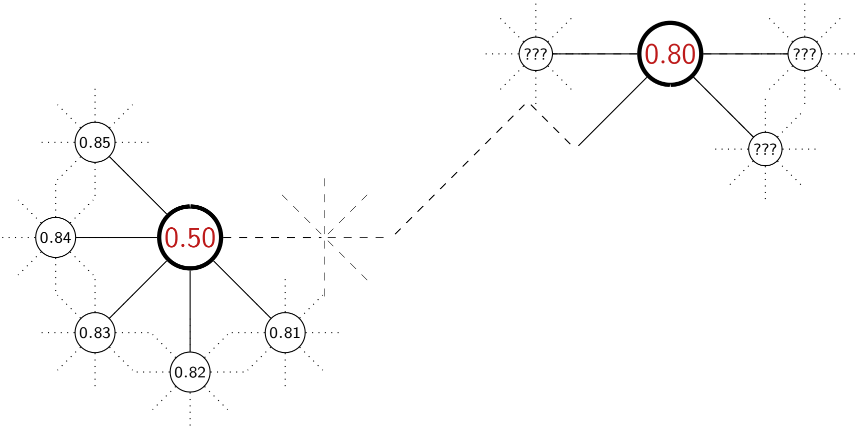
Problems

- Swap requests can't be authenticated



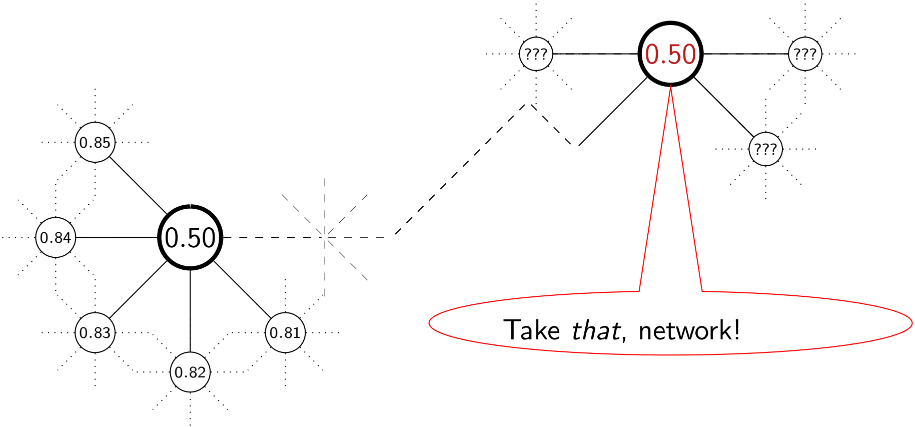
Problems

- Swap requests can't be authenticated



Problems

- Swap requests can't be authenticated



Take *that*, network!

Summary

(Reviewers can pay attention now)

- P2P computing can do more than give you free music
- Censorship is a CENSORED real threat to Internet freedom
- Freenet aims to protect freedom of speech by letting you anonymously share files in a censorship-resistant friend-to-friend network (a.k.a. "Darknet")
- Routing, storing, and retrieving data only through a network of your trusted peers can be done efficiently and in a decentralized fashion
- There are still problems

`http://freenetproject.org/`