

Anonymous communication

Tariq Elahi¹
School of Informatics
University of Edinburgh

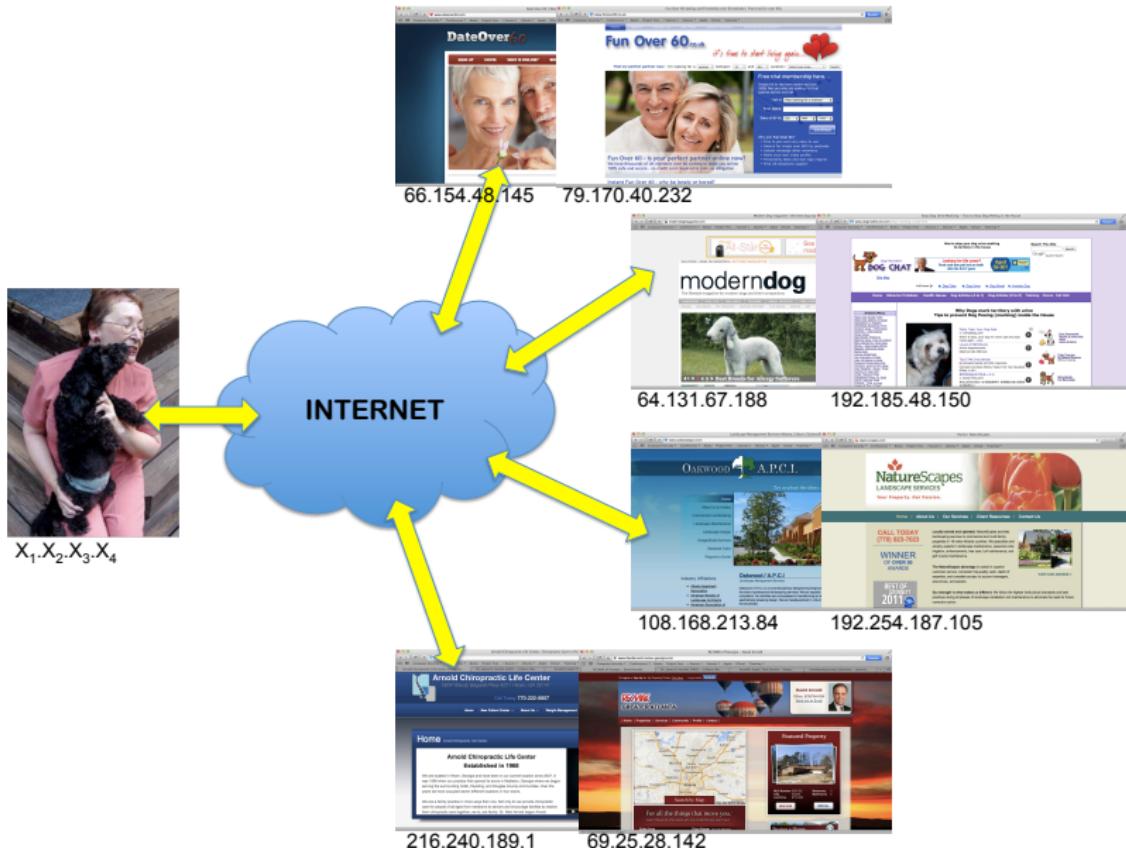
February 28, 2020

¹With slides developed by Myrto Arapinis

Context

- ▶ The Internet is a public network:
 - ▶ network routers see all traffic that passes through them
- ▶ Routing information is public:
 - ▶ IP packet headers contain source and destination of packets
- ▶ Encryption does not hide identities:
 - ▶ encryption hides payload, but not routing information

Routing information can reveal who you are!



X₁,X₂,X₃,X₄

Routing information can reveal who you are!

A Face Is Exposed for AOL Searcher No. 4417749 – New York Times

www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0

Computer Security Conferences Books Project Free ... :: Season 1 Ubuntu Apple iCloud Tutoring

HOME PAGE MY TIMES TODAY'S PAPER VIDEO MOST POPULAR TIMES TOPICS SUBSCRIBE NOW Log In Register Now

The New York Times Technology Technology All NYT Search

WORLD U.S. N.Y./REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

CAMCORDERS CAMERAS CELLPHONES COMPUTERS HANDHELDs HOME VIDEO MUSIC PERIPHERALS WI-FI

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.


Erik S. Lesser for The New York Times
Theima Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga., several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. "Those are my searches," she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an

 THE GRAND BUDAPEST HOTEL

SIGN TO E-MAIL THIS PRINT REPRINTS

More Articles in Technology >

accenture

Video Gallery Latest Thinking Ad Spotlight

The Accenture Digital Difference

Digital Business is Changing

Accenture Digital - Defining Digital Business

Daily Report: With Cloud Computing, Companies Face a Glut of Tech Choices +
Maps That Live and Evolve With Data +
Detroit, Embracing New Auto Tech Initiatives, Sets App Benchmarks

The New York Times The publication of this article is sponsored by Accenture. The editorial staff of The New York Times

Routing information can reveal who you are!

Safari File Edit View History Bookmarks Develop Window Help

What Is My IP Address? IP Address Tools and More

ComputerSecurity SimSec CSexam La cryptographie dévoilée Conferences ResearchProfiles Security-Club Teaching Tutoring

IP AddressSearch Search

What's My IP Address

How you connect to the world

MY IP IP LOOKUP SPEED TEST BLACKLIST CHECK TRACE EMAIL CHANGE IP HIDE IP IP TOOLS LEARN COMMUNITY

IP Lookup know the IP address of another computer you can find where in the world it is—and more.

Trace Email Track down the geographical location and origin of an email you received.

Hide IP Learn how to use a high-tech "proxy" to mask your real IP address on the Internet.

VPN Comparison Compare top rated VPN service providers that meet your needs and budget.

Blacklist Check Have you been blocked because of the IP address you user? Check to see here.

Speed Test Is your Internet connection up to speed? Find out for free with a quick click.

IP Tools Have the right tool for any job. That goes for your Internet connection, too.

Your IPv4 Address Is:
89.241.168.239

Your IP Details:
ISP: TalkTalk
City: Edinburgh
Region: Edinburgh
Country: United Kingdom
Don't want this known? Hide your IP details

Click for more details about 89.241.168.239

Location not accurate? Update your IP location

Learn More About This IP

Twitter Share 6.2k

This Christmas, people will search for a business like yours.

Google AdWords

Check out our new Learning Center

Learn more about IP addresses, staying safe online, general computer topics and more, including a look at IPv6.

Start Here

It's not personal — It's just your connection

Routing information can reveal who you are!



"With your permission, you give us more information about you, about your friends, and we can improve the quality of your searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."

Eric Schmidt, CEO Google, 2010

Your IP address is your ID

Your IP address is Your ID.



Your IP address leaves behind digital tracks that can be used to identify you and invade your privacy

The McNealy argument



"You have zero privacy anyway. Get over it"

Scott McNealy, CEO Sun Microsystems, 1999

The Schmidt argument



"If you have something that you don't want anyone to know maybe you shouldn't be doing it in the first place"

Eric Schmidt, CEO Google, 2009

Anonymity

Definition (ISO/IEC standard 15408)

A user may use a service or resource without disclosing the user's identity.

Anonymity

Definition (ISO/IEC standard 15408)

A user may use a service or resource without disclosing the user's identity.

→ this can be achieved by hiding one's activities among others' similar activities

- Dining cryptographers
- Crowds
- Chaum's mix
- Onion routing

Three-party dining cryptographers (3DC)

Three NSA cryptographers are having dinner. At the end of the dinner they are informed that the dinner has already been paid for. Now, either the NSA paid for the dinner, or one of the cryptographers did. They want to know if it is the NSA that paid, or one of them, **without** revealing the identity of the paying cryptographer.

3DC protocol:

1. **Phase 1:** Each pair of cryptographers flips a coin (that only they can see), where heads = 1 and tails = 0
 - ▶ each cryptographer will see two coin flips.
2. **Phase 2:** Each participant publicly announces the result as follows:
 - ▶ **Did NOT pay:** the XOR of the two coin flips they observed
 - ▶ **Did pay:** the *negation* of the XOR of the two coin flips they observed
3. **Resolution:** If the XOR of the three announcements is:
 - ▶ 0: The NSA paid
 - ▶ 1: One of them paid (but only the payer will know this.)

Superposed sending

- ▶ 3DC protocol generalises to any group size $n > 2$ (nDC)
- ▶ Sender wants to anonymously broadcast a message m . For each bit, m_i , of m :
 1. every pair of users generate a random bit (0, 1)
 - ▶ every user observes $n - 1$ bits.
 2. each user (except the sender) announces (XOR of all $n - 1$ observed bits)
 3. the sender announces (XOR of all $n - 1$ observed bits and m_i)
 4. XOR of all announcements = m_i
 - ▶ every randomly generated bit occurs in this sum twice (and is cancelled by XOR)
 - ▶ m_i occurs only once

Limitations of the DC protocol

The DC protocol is impractical:

- ▶ Requires pair-wise shared secret keys (secure channels) between the participants (to share random bits)
- ▶ Requires large amounts of randomness
- ▶ Any one can launch a denial of service attack by either not performing the protocol properly, or by transmitting at the same time as some one else. Only one person can transmit at any given round.

Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions".
ACM Transactions on Information and System Security.]

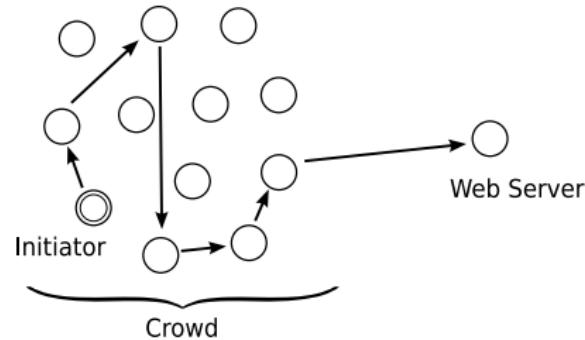
Idea: randomly route the request through a crowd of users

Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

- ▶ a crowd is a group of m users; c out of m users may be corrupted

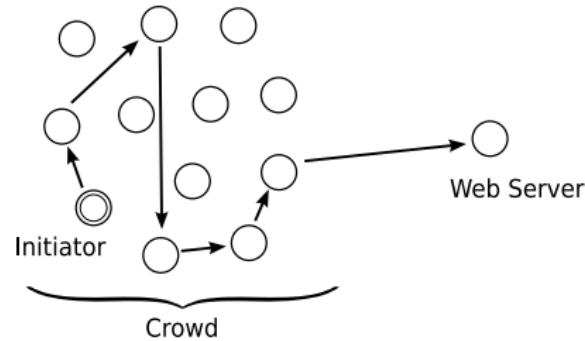


Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

- ▶ a crowd is a group of m users; c out of m users may be corrupted
- ▶ an initiator that wants to request a webpage creates a path between him and the server:

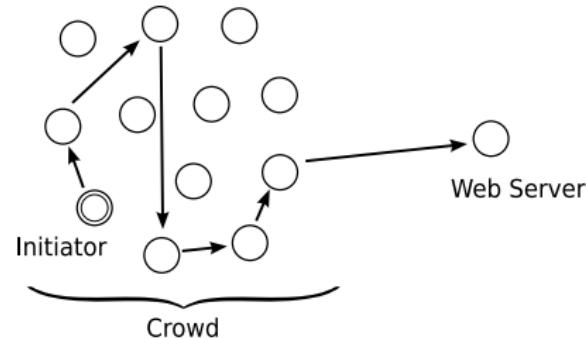


Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

- ▶ a crowd is a group of m users; c out of m users may be corrupted
- ▶ an initiator that wants to request a webpage creates a path between him and the server:
 1. the initiator selects a forwarder from the crowd and sends him his request

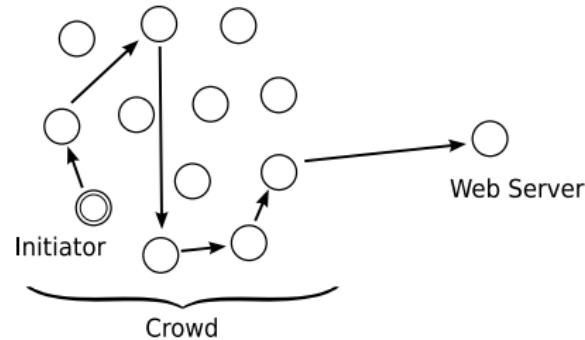


Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

- ▶ a crowd is a group of m users; c out of m users may be corrupted
- ▶ an initiator that wants to request a webpage creates a path between him and the server:
 1. the initiator selects a forwarder from the crowd and sends him his request
 2. a forwarder delivers the request directly to the server with probability $1 - p_f$; he forwards the request to a randomly selected new forwarder from the crowd with probability p_f , the new forwarder repeats the procedure

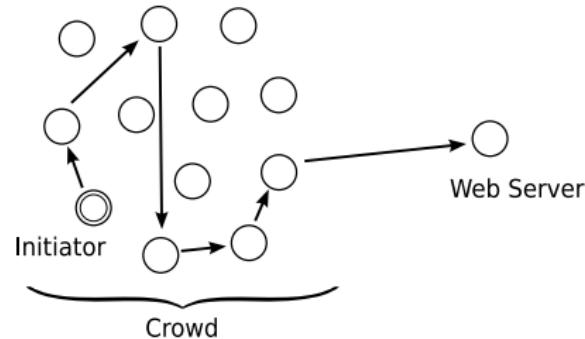


Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

- ▶ a crowd is a group of m users; c out of m users may be corrupted
- ▶ an initiator that wants to request a webpage creates a path between him and the server:
 1. the initiator selects a forwarder from the crowd and sends him his request
 2. a forwarder delivers the request directly to the server with probability $1 - p_f$; he forwards the request to a randomly selected new forwarder from the crowd with probability p_f , the new forwarder repeats the procedure
 3. the response from the server follows same route in opposite direction

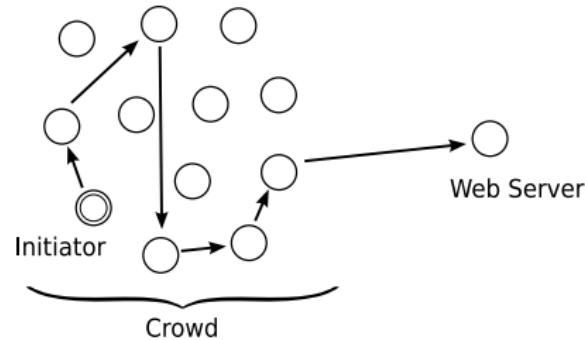


Crowds

[M. K. Reiter and A. D. Rubin, "Crowds: anonymity for Web transactions". ACM Transactions on Information and System Security.]

Idea: randomly route the request through a crowd of users

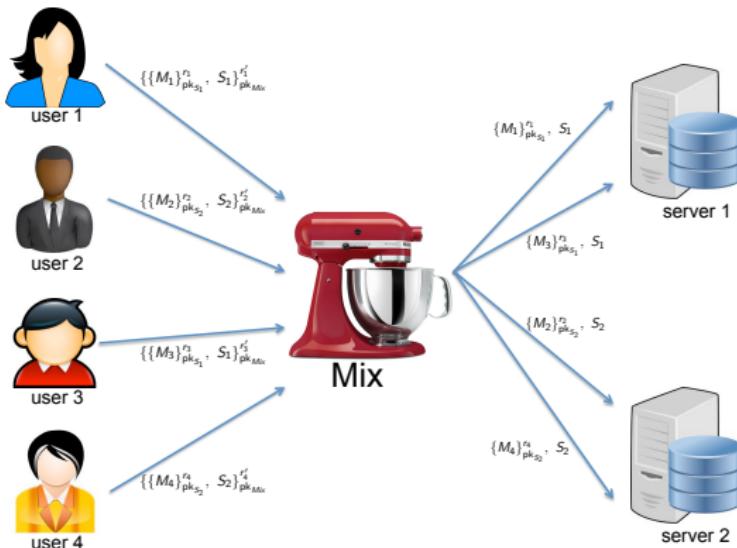
- ▶ a crowd is a group of m users; c out of m users may be corrupted
- ▶ an initiator that wants to request a webpage creates a path between him and the server:
 1. the initiator selects a forwarder from the crowd and sends him his request
 2. a forwarder delivers the request directly to the server with probability $1 - p_f$; he forwards the request to a randomly selected new forwarder from the crowd with probability p_f , the new forwarder repeats the procedure
 3. the response from the server follows same route in opposite direction



Crowd IS NOT resistant
against an attacker that sees
the whole network traffic!

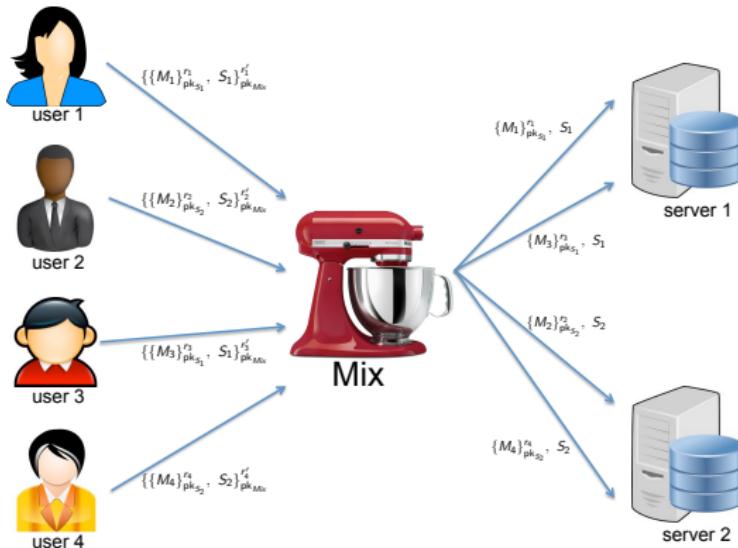
Chaum's mix

[D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, February 1981.]



Chaum's mix

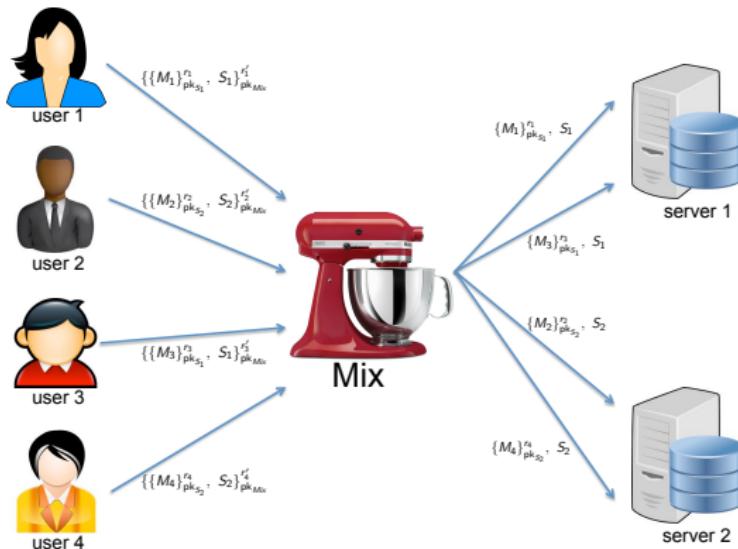
[D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, February 1981.]



- ▶ **message padding** and **buffering** to avoid time correlation attacks

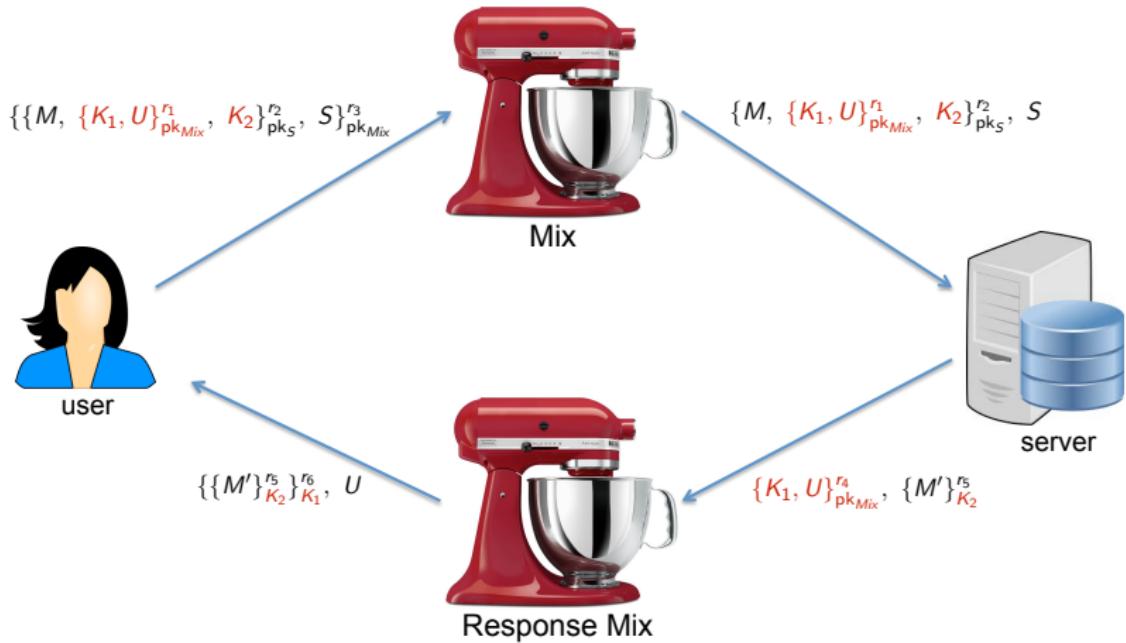
Chaum's mix

[D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM, February 1981.]

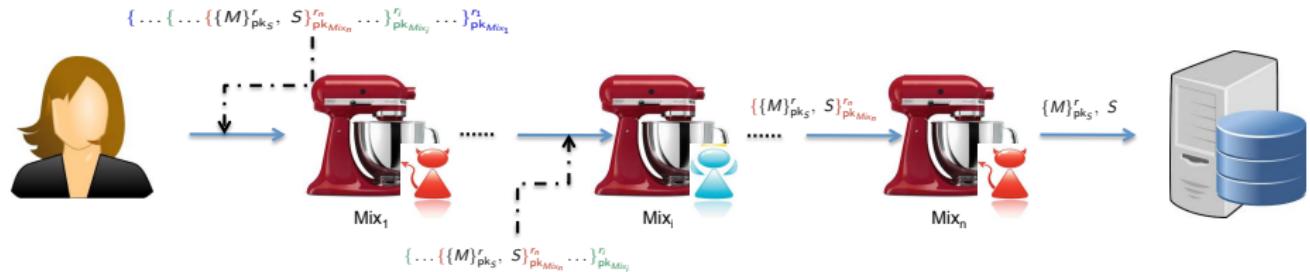


- ▶ **message padding** and **buffering** to avoid time correlation attacks
- ▶ **dummy messages** are generated by the mixes themselves to prevent an attacker sending $n - 1$ messages to a mix with capacity n , allowing him to then link the sender of the n^{th} message with its recipient

Anonymous return addresses



Mix cascade



- ▶ messages are sent through a sequence of mixes
- ▶ some of the mixes may be corrupted
- ▶ a single honest mix guarantees anonymity against an attacker controlling the whole network provided it applies:
 - ▶ message padding
 - ▶ buffering
 - ▶ dummy messages

Limitations of Chaum's mixnets

- ▶ Asymmetric encryption is not efficient
- ▶ Dummy messages are inefficient
- ▶ Buffering is not efficient