Private & Anonymous Communication

Peter Kairouz
ECE Department
University of Illinois at Urbana-Champaign
Communication

- transfer of information from one point in space-time to the other
Wireless communication

- the fundamental limits of wireless communication are well understood
Rise of the planet of the apps!
Rise of the planet of the apps!
Rise of the planet of the apps!
Rise of the planet of the apps!

can we communicate **anonymously** and **privately**?
Does privacy matter?

“if you’re doing something that you don’t want other people to know, maybe you shouldn’t be doing it in first place”

“privacy is no longer a social norm!”
Recent privacy leaks
deanonymizing Netflix data, identifying personal genomes, etc.
China’s crackdown on messaging apps

- if your message is shared 500 times, you may face 3 years in prison
Political activism

some people have important, sensitive things to say
Personal confessions

I think I'm schizophrenic... I see and hear things and I have a voice in my head, when I go to sleep it's like sleeping in a busy restaurant!

I'm a Mormon, and losing my faith.

others have less important, but sensitive things to say
Private and anonymous communication

- the data privacy and meta-data privacy contexts
Part I: Anonymous Communication
Existing anonymous messaging apps

Yik Yak

whisper

Bob

Alice

distance
Existing anonymous messaging apps

Bob

"I tried to facetime campus police last night."
Existing anonymous messaging apps

Yik Yak

whisper

"I tried to facetime campus police last night."
Existing anonymous messaging apps

Yik Yak

whisper

"I tried to facetime campus police last night."

"Attendance is not expected to be high today given the rain and hangovers."

Bob
Existing anonymous messaging apps

Yik Yak

whisper

"Attendance is not expected to be high today given the rain and hangovers."

Bob

"I tried to facetime campus police last night."
Existing anonymous messaging apps

secret

Alice
Existing anonymous messaging apps

secret

"I tried to facetime campus police last night."
Existing anonymous messaging apps

secret

"I tried to facetime campus police last night."
Existing anonymous messaging apps

secret

"I tried to facetime campus police last night."
Existing anonymous messaging apps

secret

"I tried to facetime campus police last night."
Existing anonymous messaging apps

Bob

Mary

Alice
Existing anonymous messaging apps

Bob

Mary

Alice
Existing anonymous messaging apps

Server

Bob

Alice

Mary
Existing anonymous messaging apps
Existing anonymous messaging apps

centralized networks are not truly anonymous!
Compromises in anonymity
Compromises in anonymity
Compromises in anonymity extend beyond the network.
Anonymous communication

freenet

Tor

OneSwarm

Privacy preserving peer-to-peer data sharing
Anonymous communication

freenet

Tör

OneSwarm
Privacy preserving peer-to-peer data sharing

designed for point-to-point communication
Distributed messaging
Distributed messaging

Alice

Bob

Mary
Distributed messaging

what can an adversary do?
Adversary without timing

Craig

Bob

Mary

David

Alice
Adversary without timing
Adversary without timing
adversary can figure out who got the message
Adversary with timing

- Craig
- Bob
- Mary
- David
- Alice
Adversary with timing
Adversary with timing

adversary can collect **timing information**
Adversary with timing

- message
- timestamp

adversary can collect **timing information**
Distributed network forensics

\[
\text{timing} + \text{who has the message} = \text{authorship}
\]
Information flow in social networks

- $G$ is the graph representing the social network
Information flow in social networks

message author
Information flow in social networks

- the author passes the message to its neighbors
Information flow in social networks

- its neighbors pass the message to theirs
Information flow in social networks

- the message spreads in **all directions** at the **same rate**
Information flow in social networks

- the message spreads in all directions at the same rate
Information flow in social networks

- the message spreads in all directions at the same rate
Information flow in social networks

- this spreading model is known as the diffusion model
Adversary

can we locate the message author?
Concentration around the center

- the message author is in the “center”
Node eccentricity

- maximum distance from a node to any other node
• the message author has an eccentricity of 3
Node eccentricity

- all other nodes have larger eccentricities
- other centralities: distance centrality, rumor centrality, etc.
Maximum likelihood detection

diffusion spreading = deanonymization

[Shah, Zaman 2011]
Our goal

engineer the spread to hide authorship
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion
Main Result: Adaptive diffusion

provides provable anonymity guarantees

[Spy vs. Spy: Rumor Source Obfuscation, to appear in ACM SIGMETRICS 2015]
Line graphs

- let’s start with line graphs
the message author starts a rumor at $T = 0$
Line graphs: diffusion

- with probability $p$, the left (right) node receives the message

$T = 1$
Line graphs: diffusion

- the node to the right of the author receives the message

\[ T = 1 \]
the rumor propagates in both directions at the same rate

\( T = 2 \)
Line graphs: diffusion

- the rumor propagates in both directions at the same rate

\[ T = 2 \]
Line graphs: diffusion

- $p$ is independent of time or hop distance to message author

$T = 3$
Line graphs: diffusion

- diffusion on a line is equivalent to two independent random walks

\[ T = 3 \]
Adversary

$N = 5$

nodes with the message

can we locate the message author?
Maximum likelihood detection

- the node in the middle is the mostly likely author
Maximum likelihood detection

Probability of detection $\approx \frac{1}{\sqrt{N}}$
Pólya’s urn process

- choose a ball at random from the urn

$T = 1$
Pólya’s urn process

- choose a ball at random from the urn

\[ T = 1 \]

with probability \( \frac{1}{2} \)
Pólya’s urn process

- replace the chosen ball by two balls of the same color
Pólya's urn process

- repeat previous steps

$T = 2$
Pólya’s urn process

- repeat previous steps

$T = 2$

with probability 2/3
Pólya’s urn process

the rich get richer and poor get poorer
Pólya’s urn process: anonymity properties

10 red and 4 blue

4 red and 10 blue

7 red and 7 blue

$T = 14$

all events are equally likely
Pólya’s urn process: learning

given two urns generated independently

Urn 1: 10 red and 4 blue
Urn 2: 5 red and 9 blue
Pólya’s urn process: learning

how many red balls came from urn 1?
- we broke the **concentration** around $N/2$
Line graphs: adaptive diffusion

- consider a line graph
Line graphs: adaptive diffusion

- node 0 starts a rumor at $T = 0$
Line graphs: adaptive diffusion

- with probability $\frac{1}{2}$, the left (right) node receives the message
Line graphs: adaptive diffusion

- right node 1 receives the message
Line graphs: adaptive diffusion

- probability of passing message = \( \frac{h+1}{T+1} \)

\[ T = 2 \]

hop distance to message author

elapsed time
Line graphs: adaptive diffusion

- right node 2 receives the message
Line graphs: *adaptive diffusion*

- Probability of passing message: \( \frac{h+1}{T+1} \)
- Hop distance to message author
- Elapsed time

\[ T = 3 \]
Line graphs: adaptive diffusion

- left node 1 receives the message

\[ T = 3 \]
Adversary

$N = 4$ nodes with the message

can we locate the message author?
Maximum likelihood detection

Likelihoods

diffusion

adaptive diffusion
Maximum likelihood detection

Probability of detection $\approx \frac{1}{N}$
$d$-regular trees

- what about $d$-regular trees?
$d$-regular trees: diffusion

- likelihoods concentrate around the center
$d$-regular trees: Pólya’s urn processes

Probability of detection using Jordan centrality

- does not work at all!
$d$-regular trees: adaptive diffusion
$d$-regular trees: adaptive diffusion

- Initially, the author is also the "virtual source"
\(d\)-regular trees: adaptive diffusion

- at \(T = 1\), the author selects one neighbor at random
$d$-regular trees: adaptive diffusion

- at $T = 1$, the author selects one neighbor at random

the author passes $h = 1$ and $T = 2$ to the chosen neighbor
$d$-regular trees: adaptive diffusion

- the chosen neighbor becomes the new virtual source
$d$-regular trees: adaptive diffusion

- at $T = 2$, the virtual source passes the message to all its neighbors
\(d\)-regular trees: adaptive diffusion

- as \(T\) transitions from even to odd, the virtual source has two options:
  - keeping the virtual source token
  - passing the virtual source token
Keeping the virtual source token

- virtual source token is kept with probability \[ \frac{(d-1)^{\frac{T}{2}-h-1}-1}{(d-1)^{\frac{T}{2}+1}-1} \]
Keeping the virtual source token

- all leaf nodes with the message pass it to their neighbors

happens in $T = 3$ and $T = 4$
Passing the virtual source token

- current virtual source selects one of its neighbors at random
Passing the virtual source token

- current virtual source selects one of its neighbors at random

- current virtual source passes $h = 2$ and $T = 4$ to new virtual source
Passing the virtual source token

- new virtual source passes the message to its neighbors which in turn pass it to their neighbors

happens in $T = 3$ and $T = 4$
the graph is *always symmetric* around the *virtual source*
Adversary

can we locate the message author?
Maximum likelihood detection

- **all nodes** except for the final virtual source are equally likely
Maximum likelihood detection

Probability of detection = $\frac{1}{N-1}$
General graphs

can we extend adaptive diffusion for general graphs?
General graphs: *cycles*

- do not pass the message to a node that already has the message
virtual source token is kept with probability

\[
\frac{(d-1)^{\frac{T}{2}-h-1} - 1}{(d-1)^{T+1} - 1}
\]
General graphs: degree irregularities

- any $d \geq 3$ works well in practice
- to preserve symmetry, each node talks to at most 3 neighbors
General graphs: **boundary effects**

- the **virtual source** is allowed to turn around when it hits the boundary
Simulation setup

- 10,000 Facebook users in New Orleans circa 2009
- All users with degree less than 3 were removed
Simulation results

- on average, 96% of users received the message within 10 time steps
Simulation results

- likelihoods can be approximated numerically
Part I: Proposed Research
Spy adversarial model

adversary can collect timing information
Adversary with timing

what if spies can collect timing information?

spy node 1

.sparse node 2

$N = \text{distance between spies}$
Maximum likelihood detection

Probability of detection

hop distance between spies

Probability of detection \( \approx \frac{1}{N} \)
Adversary with timing

cordon of spy nodes: a work in progress
Current progress: Wildfire
Current progress: *Wildfire*

Wildfire empowers devices by removing central service providers.
Current progress: Wildfire

Wildfire empowers devices by removing central service providers
Wildfire empowers devices by removing central service providers. It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.
Wildfire empowers devices by removing central service providers. It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.
Wildfire empowers devices by removing central service providers. It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.
Wildfire empowers devices by removing central service providers. It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.
Current progress: **Wildfire**

Wildfire empowers devices by removing central service providers. It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

Anonymous, distributed, secure implementation.
Upcoming research

Theoretical

• Spy adversarial model
• Hiding relays
• Dynamic networks

Systems

• Video sharing
• Message caching
• Bootstrapping contacts

Wildfire Release
Part II: Private Communication
Local privacy model

- clients receive a service if they share their data
- clients do not trust data analyst
Lying is the ultimate protection

“the future of privacy is lying”

- lying = randomizing
Privacy via plausible deniability

have you ever used illegal drugs?

say yes

answer truthfully

[Warner 1965]
Privacy via plausible deniability

- instead of $X = x$, share $Y = y$ w.p. $Q(y|x)$
- $Q: |X| \times |Y|$ is a stochastic mapping
Local privacy model

- each user **privatizes** her data before releasing it

[Duchi, et. al., 2013]
Local differential privacy

$Q$ is $\epsilon$-locally differentially private iff for all $x, x' \in X$ and $y \in Y$

$$e^{-\epsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\epsilon}$$

$\epsilon$ controls the level of privacy
- large $\epsilon$, low privacy
- small $\epsilon$, high privacy

- $\mathcal{D}_\epsilon$: set of all $\epsilon$-locally differentially private mechanisms
Privacy vs utility

- the more private you want to be, the less utility you get
- there is a fundamental trade-off between privacy and utility

\[
\begin{align*}
\text{maximize} & \quad U(Q) \\
\text{subject to} & \quad Q \in D_\varepsilon
\end{align*}
\]

$U(Q)$: application dependent utility function

$D_\varepsilon$: set of all $\varepsilon$-locally differentially private mechanisms
Utility functions obeying the data processing inequality:

\[ T = Q \circ W \Rightarrow U(T) \leq U(Q) \]

- further randomization can only reduce utility
- note that if \( Q \in \mathcal{D}_\epsilon \Rightarrow T \in \mathcal{D}_\epsilon \)
Information theoretic utility functions

- for $|\mathcal{X}| > 2$, we focus on a rich class of convex utility functions:

\[
\begin{align*}
\text{maximize} & \quad U(Q) = \sum_{y \in \mathcal{Y}} \mu(Q_y) \\
\text{subject to} & \quad Q \in D_{\varepsilon}
\end{align*}
\]

$Q_y$: the column of $Q$ corresponding to $Q(y|.)$

$\mu$: any sub-linear function

includes all $f$-divergences and mutual information
Staircase mechanisms

$Q$ is $\varepsilon$-locally differentially private if for all $x, x' \in X$ and $y \in Y$

$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$
Staircase mechanisms

$Q$ is $\varepsilon$-locally differentially private if for all $x, x' \in X$ and $y \in Y$

$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^\varepsilon$$

$Q$ is a staircase mechanism if for all $x, x' \in X$ and $y \in Y$

$$\frac{Q(y|x)}{Q(y|x')} \in \{e^{-\varepsilon}, 1, e^\varepsilon\}$$
Example of staircase mechanisms

\[ Q^T = \frac{1}{1+e^\varepsilon} \begin{bmatrix} e^\varepsilon & e^\varepsilon & 1 & e^\varepsilon & 1 \\ 1 & 1 & e^\varepsilon & 1 & e^\varepsilon \end{bmatrix} \]

\[ Q^T = \frac{1}{3+e^\varepsilon} \begin{bmatrix} e^\varepsilon & 1 & 1 & 1 \\ 1 & e^\varepsilon & 1 & 1 \\ 1 & 1 & e^\varepsilon & 1 \\ 1 & 1 & 1 & e^\varepsilon \end{bmatrix} \]

Binary Mechanism

Randomized Response
Main result: binary data

for $|\mathcal{X}| = 2$, binary data:

- w.p. $\frac{1}{1+e^\varepsilon}$ lie
- w.p. $\frac{e^\varepsilon}{1+e^\varepsilon}$ say the truth

- optimal for all $\varepsilon$
- optimal for all $U(Q)$ obeying the data processing inequality
Main result: general case

for $|\mathcal{X}| > 2$, general data:

- staircase mechanisms are optimal for all $\varepsilon$
- BM optimal for small $\varepsilon$
- RR optimal for large $\varepsilon$
Acknowledgments

Giulia Fanti
Pramod Viswanath
Sewoong Oh
Thank You!