How to do Research

This is as much discussion as presentation so please interrupt!

Roadmap

Research Style

Choosing and Refining Ideas

Finding/Reading Academic Papers

Project Scale and Prior Work

Collaboration

Please don’t make us go to court

Research Style

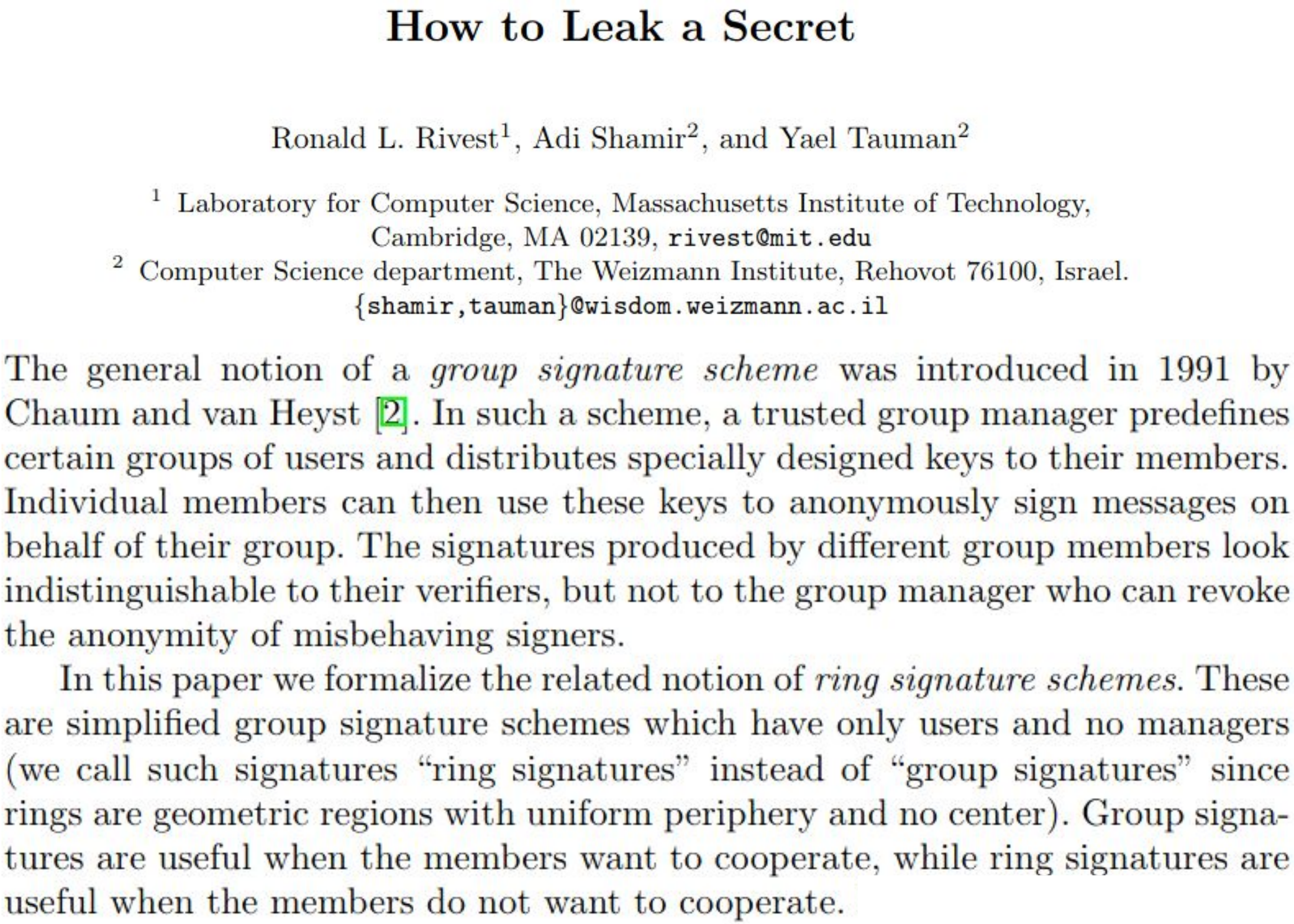
Two main “kinds” of security research

1. Theory
   a. Furthers *understanding*
2. Systems
   a. Addresses a *problem*

Paper introduction tone:

Systems papers focus on resolving some issue present in the world while theory papers focus on resolving a gap in our knowledge.

Most of the projects in this class will be *systems*



How to Leak a Secret

Ronald L. Rivest[1], Adi Shamir[2], and Yael Tauman[2]

[1] Laboratory for Computer Science, Massachusetts Institute of Technology,
Cambridge, MA 02139, rivest@mit.edu
[2] Computer Science department, The Weizmann Institute, Rehovot 76100, Israel.
{shamir,tauman}@wisdom.weizmann.ac.il

The general notion of a *group signature scheme* was introduced in 1991 by Chaum and van Heyst [2]. In such a scheme, a trusted group manager predefines certain groups of users and distributes specially designed keys to their members. Individual members can then use these keys to anonymously sign messages on behalf of their group. The signatures produced by different group members look indistinguishable to their verifiers, but not to the group manager who can revoke the anonymity of misbehaving signers.

In this paper we formalize the related notion of *ring signature schemes*. These are simplified group signature schemes which have only users and no managers (we call such signatures "ring signatures" instead of "group signatures" since rings are geometric regions with uniform periphery and no center). Group signatures are useful when the members want to cooperate, while ring signatures are useful when the members do not want to cooperate.

Prio: Private, Robust, and Scalable Computation of Aggregate Statistics

Henry Corrigan-Gibbs and Dan Boneh
Stanford University

Our smartphones, cars, and wearable electronics are constantly sending telemetry data and other sensor readings back to cloud services. With these data in hand, a cloud service can compute useful *aggregate statistics* over the entire population of devices. For example, navigation app providers collect real-time location data from their users to identify areas of traffic congestion in a city and route drivers along the least-crowded roads [80]. Fitness tracking services collect information on their users' physical activity so that each user can see how her fitness regimen compares to the average [75]. Web browser vendors collect lists of unusually popular homepages to detect homepage-hijacking adware [57].

Even when a cloud service is only interested in learning aggregate statistics about its user population as a whole, such services often end up collecting private data from each client and storing it for aggregation later on. These centralized caches of private user data pose severe security and privacy risks: motivated attackers may steal and disclose clients' sensitive information [84, 117], cloud services may misuse the clients' information for profit [112], and intelligence agencies may appropriate the data for targeting or mass surveillance purposes [65].

Choosing Project Ideas

- What do you 🖤 ?
  - Hobbies? Your favorite class?
  - Security is ***everywhere***

Choosing Project Ideas

- What do you 🖤 ?
    - Hobbies? Your favorite class?
    - Security is ***everywhere***
- What do you use?
    - Do you understand how the devices around you work?
        - How does your computer know what time it is?
        - Caller ID???
        - The unlock button on a car remote?

Choosing Project Ideas

- What do you 🖤 ?
  - Hobbies? Your favorite class?
  - Security is ***everywhere***
- What do you use?
  - Do you understand how the devices around you work?
    - How does your computer know what time it is?
    - Caller ID???
    - The unlock button on a car remote?
- What is exciting?
  - If you aren’t excited about your project, no one else will be either

Choosing Project Ideas

- What do you 🖤 ?
    - Hobbies? Your favorite class?
    - Security is ***everywhere***
- What do you use?
    - Do you understand how the devices around you work?
        - How does your computer know what time it is?
        - Caller ID???
        - The unlock button on a car remote?
- What is exciting?
    - If you aren’t excited about your project, no one else will be either
- Do you **enjoy** the type of work you’re about to sign up for?
    - When you consider a topic, think about how you’ll reach your result, not just about the result itself! Programming? Reverse engineering?

Refining your Topic

What problem are you solving?

Why is this an important problem?

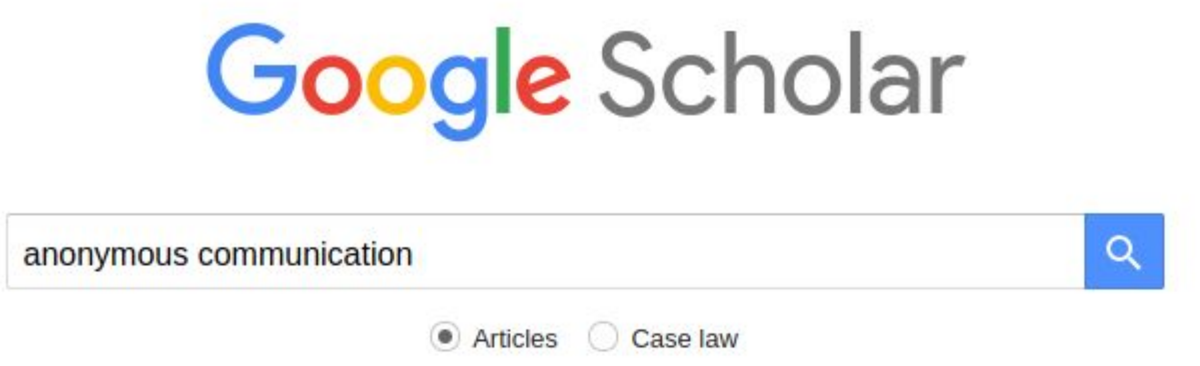
What other work exists in the area?

What are the limitations of your approach?

How to Find Papers

scholar.google.com

How to Find Papers



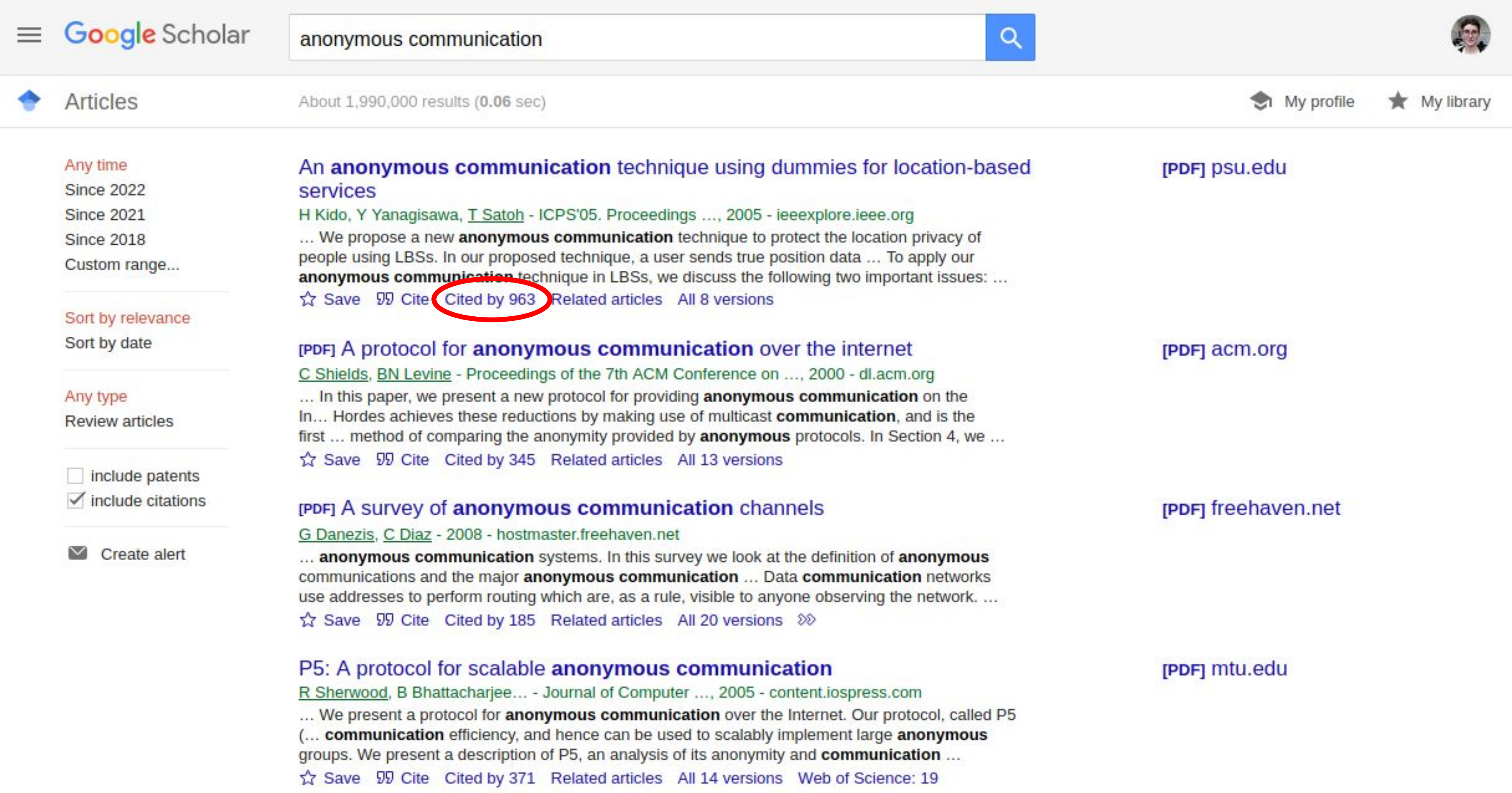
anonymous communication

● Articles ○ Case law

How to Find Papers

Cited by

- Generally corresponds to “influence”
- Look at works citing a paper to find similar followup works!



About 1,990,000 results (**0.06** sec)

An **anonymous communication** technique using dummies for location-based services — [PDF] psu.edu

H Kido, Y Yanagisawa, T Satoh - ICPS'05. Proceedings …, 2005 - ieeexplore.ieee.org

… We propose a new **anonymous communication** technique to protect the location privacy of people using LBSs. In our proposed technique, a user sends true position data … To apply our **anonymous communication** technique in LBSs, we discuss the following two important issues: …

☆ Save 99 Cite Cited by 963 Related articles All 8 versions

[PDF] A protocol for **anonymous communication** over the internet — [PDF] acm.org

C Shields, BN Levine - Proceedings of the 7th ACM Conference on …, 2000 - dl.acm.org

… In this paper, we present a new protocol for providing **anonymous communication** on the In… Hordes achieves these reductions by making use of multicast **communication**, and is the first … method of comparing the anonymity provided by **anonymous** protocols. In Section 4, we …

☆ Save 99 Cite Cited by 345 Related articles All 13 versions

[PDF] A survey of **anonymous communication** channels — [PDF] freehaven.net

G Danezis, C Diaz - 2008 - hostmaster.freehaven.net

… **anonymous communication** systems. In this survey we look at the definition of **anonymous** communications and the major **anonymous communication** … Data **communication** networks use addresses to perform routing which are, as a rule, visible to anyone observing the network. …

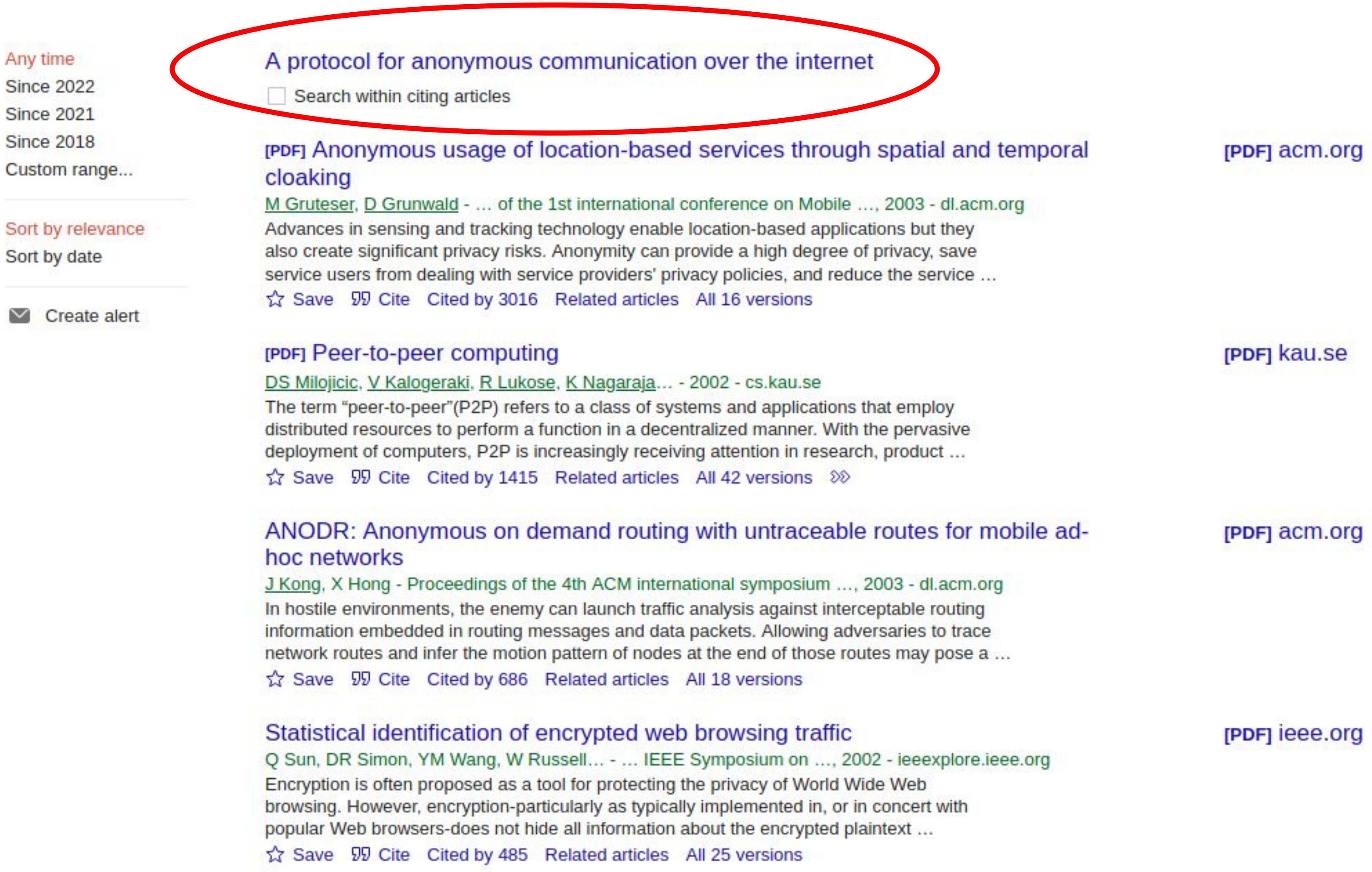
☆ Save 99 Cite Cited by 185 Related articles All 20 versions »

P5: A protocol for scalable **anonymous communication** — [PDF] mtu.edu

R Sherwood, B Bhattacharjee… - Journal of Computer …, 2005 - content.iospress.com

… We present a protocol for **anonymous communication** over the Internet. Our protocol, called P5 (… **communication** efficiency, and hence can be used to scalably implement large **anonymous** groups. We present a description of P5, an analysis of its anonymity and **communication** …

☆ Save 99 Cite Cited by 371 Related articles All 14 versions Web of Science: 19



A protocol for anonymous communication over the internet

□ Search within citing articles

[PDF] Anonymous usage of location-based services through spatial and temporal cloaking

[PDF] acm.org

M Gruteser, D Grunwald - … of the 1st international conference on Mobile …, 2003 - dl.acm.org

Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service …

☆ Save Cite Cited by 3016 Related articles All 16 versions

[PDF] Peer-to-peer computing

[PDF] kau.se

DS Milojicic, V Kalogeraki, R Lukose, K Nagaraja… - 2002 - cs.kau.se

The term "peer-to-peer"(P2P) refers to a class of systems and applications that employ distributed resources to perform a function in a decentralized manner. With the pervasive deployment of computers, P2P is increasingly receiving attention in research, product …

☆ Save Cite Cited by 1415 Related articles All 42 versions

ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks

[PDF] acm.org

J Kong, X Hong - Proceedings of the 4th ACM international symposium …, 2003 - dl.acm.org

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a …

☆ Save Cite Cited by 686 Related articles All 18 versions

Statistical identification of encrypted web browsing traffic

[PDF] ieee.org

Q Sun, DR Simon, YM Wang, W Russell… - … IEEE Symposium on …, 2002 - ieeexplore.ieee.org

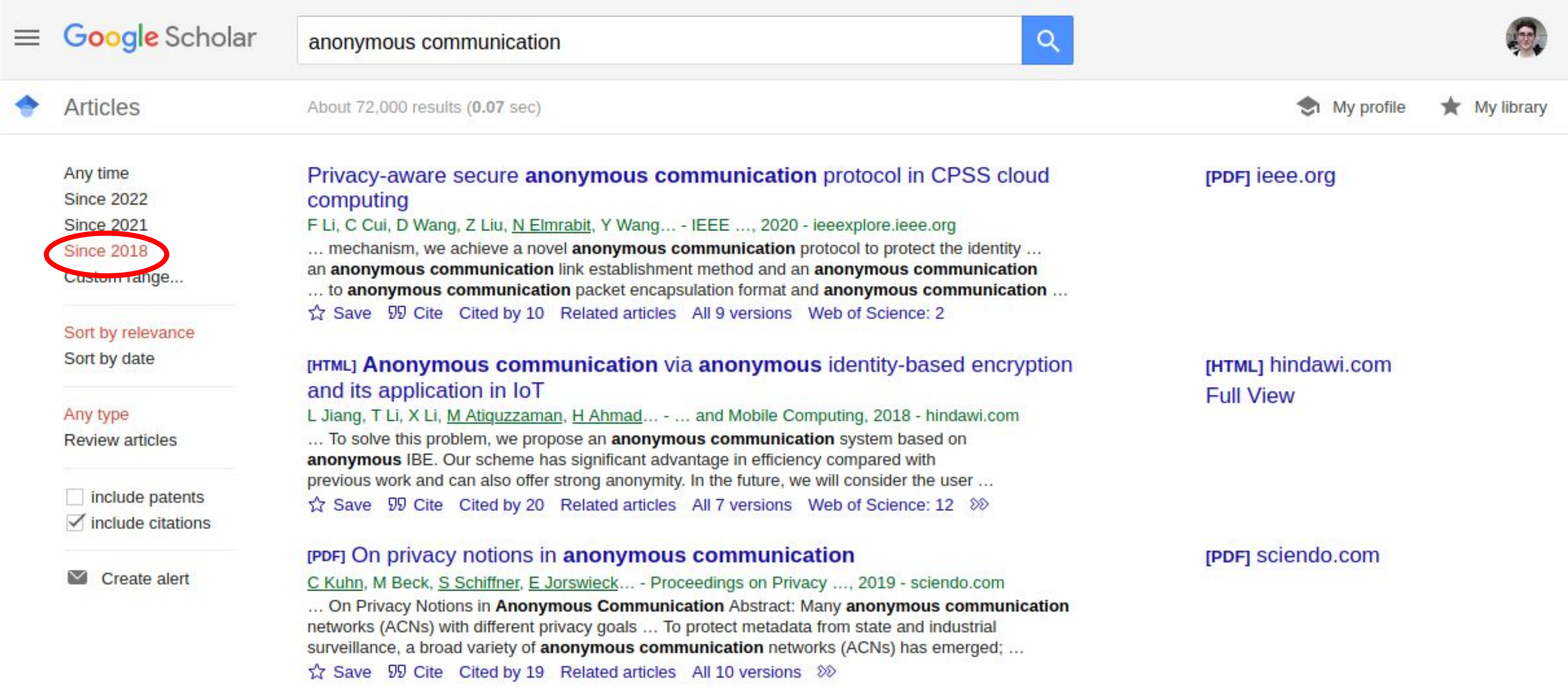
Encryption is often proposed as a tool for protecting the privacy of World Wide Web browsing. However, encryption-particularly as typically implemented in, or in concert with popular Web browsers-does not hide all information about the encrypted plaintext …

☆ Save Cite Cited by 485 Related articles All 25 versions

How to Find Papers

Year

- Old =/= bad, but newer papers will give a better view of the *current* state of the area
- It can be helpful to start with new and work back



Google Scholar

anonymous communication

Articles

About 72,000 results (**0.07** sec)

My profile

My library

Any time
Since 2022
Since 2021
[✓ Since 2018]
Custom range...

Sort by relevance
Sort by date

Any type
Review articles

□ include patents
☑ include citations

Create alert

Privacy-aware secure **anonymous communication** protocol in CPSS cloud computing

F Li, C Cui, D Wang, Z Liu, N Elmrabit, Y Wang... - IEEE ..., 2020 - ieeexplore.ieee.org

... mechanism, we achieve a novel **anonymous communication** protocol to protect the identity ... an **anonymous communication** link establishment method and an **anonymous communication** ... to **anonymous communication** packet encapsulation format and **anonymous communication** ...

☆ Save 99 Cite Cited by 10 Related articles All 9 versions Web of Science: 2

[PDF] ieee.org

[HTML] **Anonymous communication** via **anonymous** identity-based encryption and its application in IoT

L Jiang, T Li, X Li, M Atiquzzaman, H Ahmad... - ... and Mobile Computing, 2018 - hindawi.com

... To solve this problem, we propose an **anonymous communication** system based on **anonymous** IBE. Our scheme has significant advantage in efficiency compared with previous work and can also offer strong anonymity. In the future, we will consider the user ...

☆ Save 99 Cite Cited by 20 Related articles All 7 versions Web of Science: 12 »

[HTML] hindawi.com
Full View

[PDF] On privacy notions in **anonymous communication**

C Kuhn, M Beck, S Schiffner, E Jorswieck... - Proceedings on Privacy ..., 2019 - sciendo.com

... On Privacy Notions in **Anonymous Communication** Abstract: Many **anonymous communication** networks (ACNs) with different privacy goals ... To protect metadata from state and industrial surveillance, a broad variety of **anonymous communication** networks (ACNs) has emerged; ...

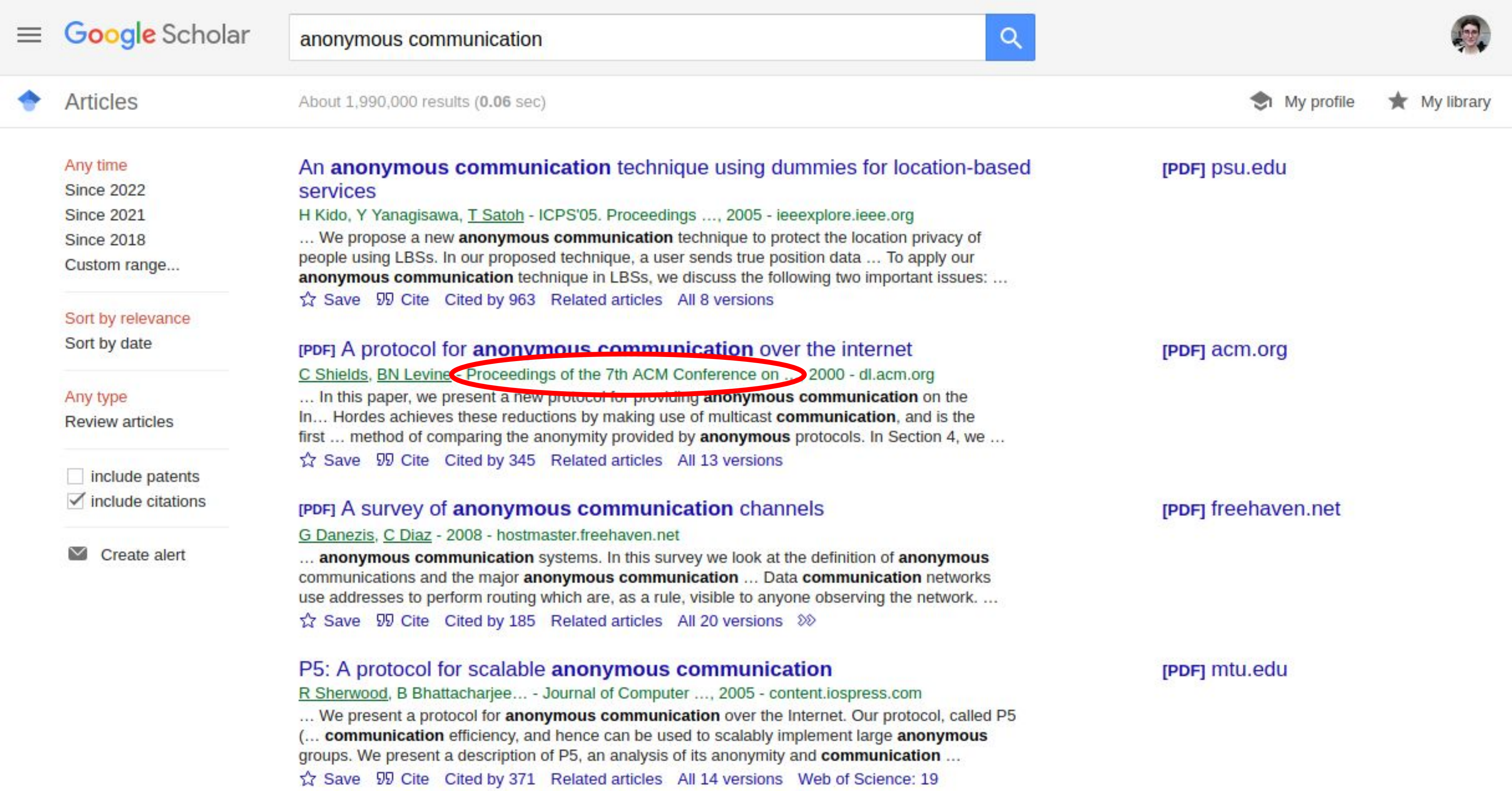
☆ Save 99 Cite Cited by 19 Related articles All 10 versions »

[PDF] sciendo.com

How to Find Papers

Conference tier

- Top tier conferences are pickier about what they accept
  - USENIX, S&P, CCS, NDSS, RWC
  - Crypto, TCC, EUROCRYPT
  - OSDI, SOSP, NSDI



Google Scholar

anonymous communication

Articles

About 1,990,000 results (**0.06** sec)

My profile

★ My library

Any time

Since 2022

Since 2021

Since 2018

Custom range...

Sort by relevance

Sort by date

Any type

Review articles

□ include patents

☑ include citations

Create alert

An **anonymous communication** technique using dummies for location-based services

H Kido, Y Yanagisawa, T Satoh - ICPS'05. Proceedings …, 2005 - ieeexplore.ieee.org

… We propose a new **anonymous communication** technique to protect the location privacy of people using LBSs. In our proposed technique, a user sends true position data … To apply our **anonymous communication** technique in LBSs, we discuss the following two important issues: …

☆ Save Cite Cited by 963 Related articles All 8 versions

[PDF] psu.edu

[PDF] A protocol for **anonymous communication** over the internet

C Shields, BN Levine - Proceedings of the 7th ACM Conference on …, 2000 - dl.acm.org

… In this paper, we present a new protocol for providing **anonymous communication** on the In… Hordes achieves these reductions by making use of multicast **communication**, and is the first … method of comparing the anonymity provided by **anonymous** protocols. In Section 4, we …

☆ Save Cite Cited by 345 Related articles All 13 versions

[PDF] acm.org

[PDF] A survey of **anonymous communication** channels

G Danezis, C Diaz - 2008 - hostmaster.freehaven.net

… **anonymous communication** systems. In this survey we look at the definition of **anonymous** communications and the major **anonymous communication** … Data **communication** networks use addresses to perform routing which are, as a rule, visible to anyone observing the network. …

☆ Save Cite Cited by 185 Related articles All 20 versions

[PDF] freehaven.net

P5: A protocol for scalable **anonymous communication**

R Sherwood, B Bhattacharjee… - Journal of Computer …, 2005 - content.iospress.com

… We present a protocol for **anonymous communication** over the Internet. Our protocol, called P5 (… **communication** efficiency, and hence can be used to scalably implement large **anonymous** groups. We present a description of P5, an analysis of its anonymity and **communication** …

☆ Save Cite Cited by 371 Related articles All 14 versions Web of Science: 19

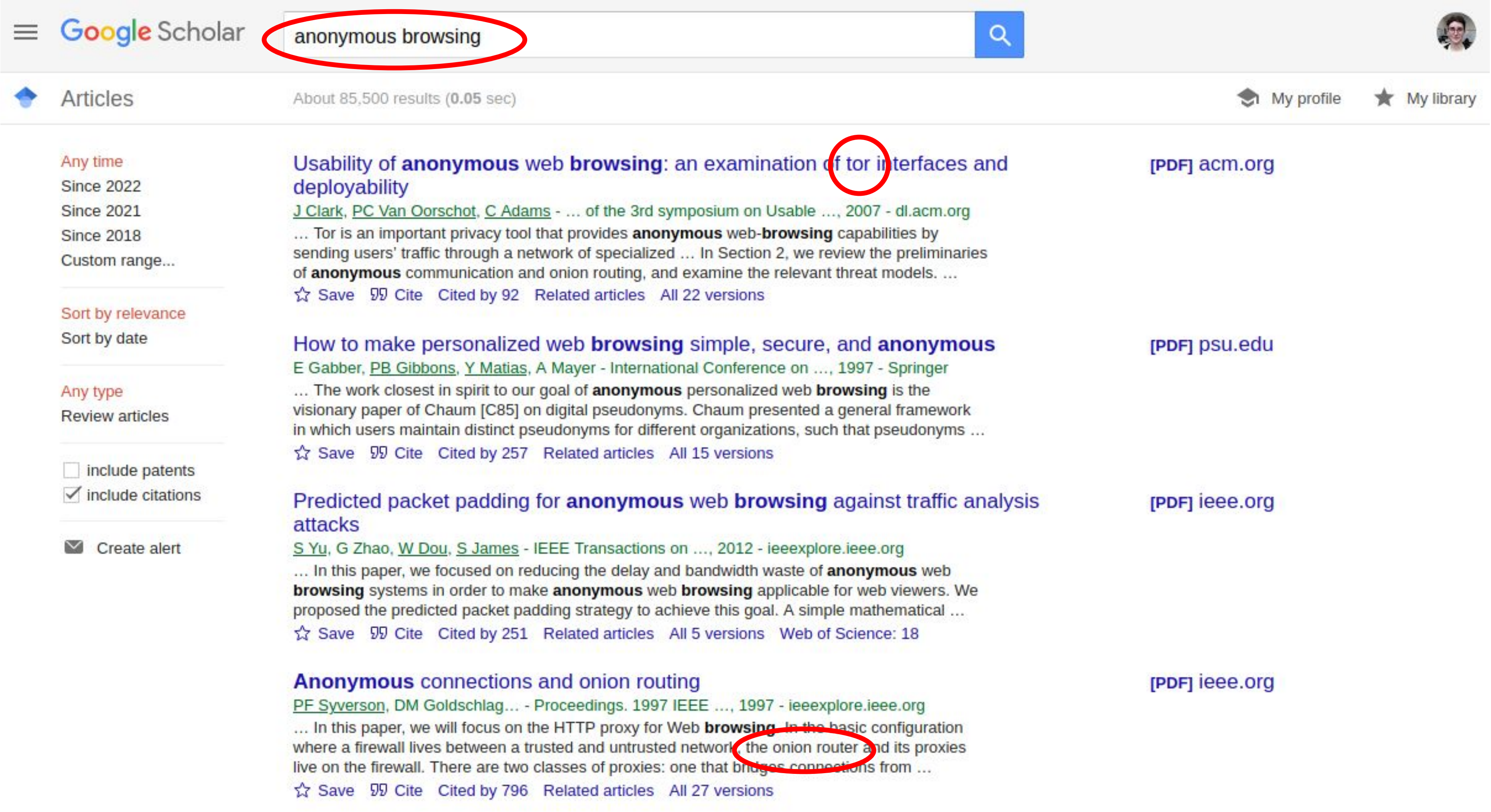
[PDF] mtu.edu

How to Find Papers

Termanology

- Google Scholar is very picky about your word choices
  - (this is a feature not a bug)
  - You need to try many different search queries when searching for papers

Where was Tor is my anonymous communication searches? (not there)



anonymous browsing

About 85,500 results (**0.05** sec)

Usability of **anonymous** web **browsing**: an examination of tor interfaces and deployability

[PDF] acm.org

J Clark, PC Van Oorschot, C Adams - … of the 3rd symposium on Usable …, 2007 - dl.acm.org

… Tor is an important privacy tool that provides **anonymous** web-**browsing** capabilities by sending users' traffic through a network of specialized … In Section 2, we review the preliminaries of **anonymous** communication and onion routing, and examine the relevant threat models. …

☆ Save 99 Cite Cited by 92 Related articles All 22 versions

How to make personalized web **browsing** simple, secure, and **anonymous**

[PDF] psu.edu

E Gabber, PB Gibbons, Y Matias, A Mayer - International Conference on …, 1997 - Springer

… The work closest in spirit to our goal of **anonymous** personalized web **browsing** is the visionary paper of Chaum [C85] on digital pseudonyms. Chaum presented a general framework in which users maintain distinct pseudonyms for different organizations, such that pseudonyms …

☆ Save 99 Cite Cited by 257 Related articles All 15 versions

Predicted packet padding for **anonymous** web **browsing** against traffic analysis attacks

[PDF] ieee.org

S Yu, G Zhao, W Dou, S James - IEEE Transactions on …, 2012 - ieeexplore.ieee.org

… In this paper, we focused on reducing the delay and bandwidth waste of **anonymous** web **browsing** systems in order to make **anonymous** web **browsing** applicable for web viewers. We proposed the predicted packet padding strategy to achieve this goal. A simple mathematical …

☆ Save 99 Cite Cited by 251 Related articles All 5 versions Web of Science: 18

Anonymous connections and onion routing

[PDF] ieee.org

PF Syverson, DM Goldschlag… - Proceedings. 1997 IEEE …, 1997 - ieeexplore.ieee.org

… In this paper, we will focus on the HTTP proxy for Web **browsing**. In the basic configuration where a firewall lives between a trusted and untrusted network, the onion router and its proxies live on the firewall. There are two classes of proxies: one that bridges connections from …

☆ Save 99 Cite Cited by 796 Related articles All 27 versions

How to Read Papers

Don’t read the whole thing top to bottom as soon as you find it!!!

1. Read the abstract
   a. Does it still seem relevant?
2. Read the introduction
   a. This will be a summary of the paper’s contributions along with its motivation
   b. Does the paper still seem relevant?
3. Read the related works
   a. This is where you find other papers in the area (and why this paper thinks they didn’t solve the problem)
   b. Find papers that cite this paper in *their* related works to see what might have been missed
4. Read the rest of the paper (optional)
   a. You should be reading full papers for works closely related to yours

Refining your Topic

What problem are you solving?

Anonymous communication is pretty slow

Refining your Topic

What problem are you solving?

Anonymous communication is pretty slow

Why is this an important problem?

People won’t use it if it’s slow

Refining your Topic

What problem are you solving?

Anonymous communication is pretty slow

Why is this an important problem?

People won’t use it if it’s slow

What other work exists in the area?

Tor: more usable than academic works, but not as strong anonymity

Refining your Topic

What problem are you solving?

Anonymous communication is pretty slow

Why is this an important problem?

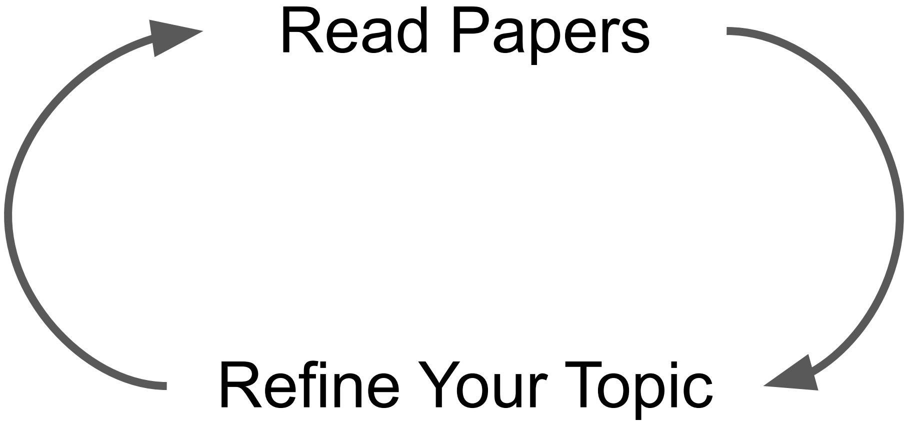
People won’t use it if it’s slow

What other work exists in the area?

Tor: more usable than academic works, but not as strong anonymity

What are the limitations of your approach?

Better performance often means worse security



Read Papers

Refine Your Topic

Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
    - See related work or, if present, “limitations”
- Is there a related problem that seems open?

Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
  - See related work or, if present, “limitations”
- Is there a related problem that seems open?

Scope: Your project is out of scope for a course project

- Any bite sized pieces you can break off?

Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
    - See related work or, if present, “limitations”
- Is there a related problem that seems open?

Scope: Your project is out of scope for a course project

- Any bite sized pieces you can break off?

Binary Projects: Your problem is either “solved” or “unsolved” with no middle ground

- You want steps along the way
    - Checkpoints along the way should be meaningful in their own right
    - Move the goalposts
    - See: Papers with titles of the format “Towards….”

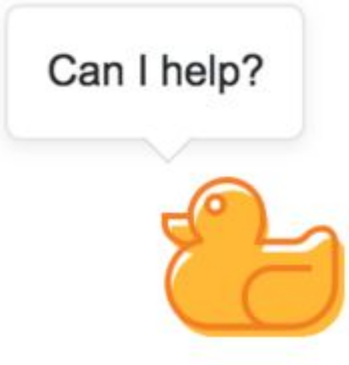
Collaboration

Research is best with friends

This is how you will refine your ideas and find bugs

It’s easy to get into the weeds and lose sight of the big picture.

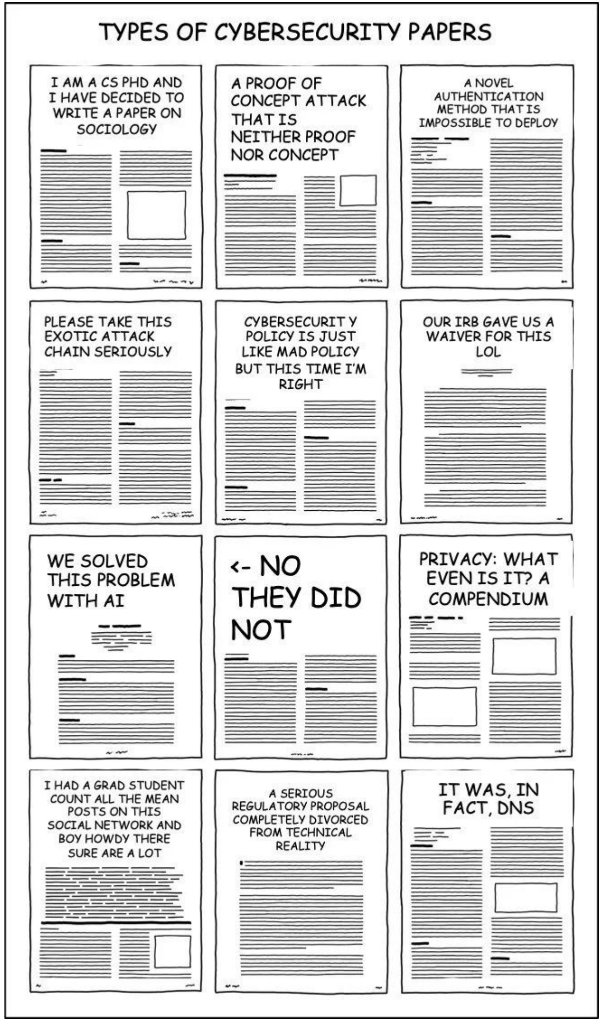
A fresh brain will catch things you missed.



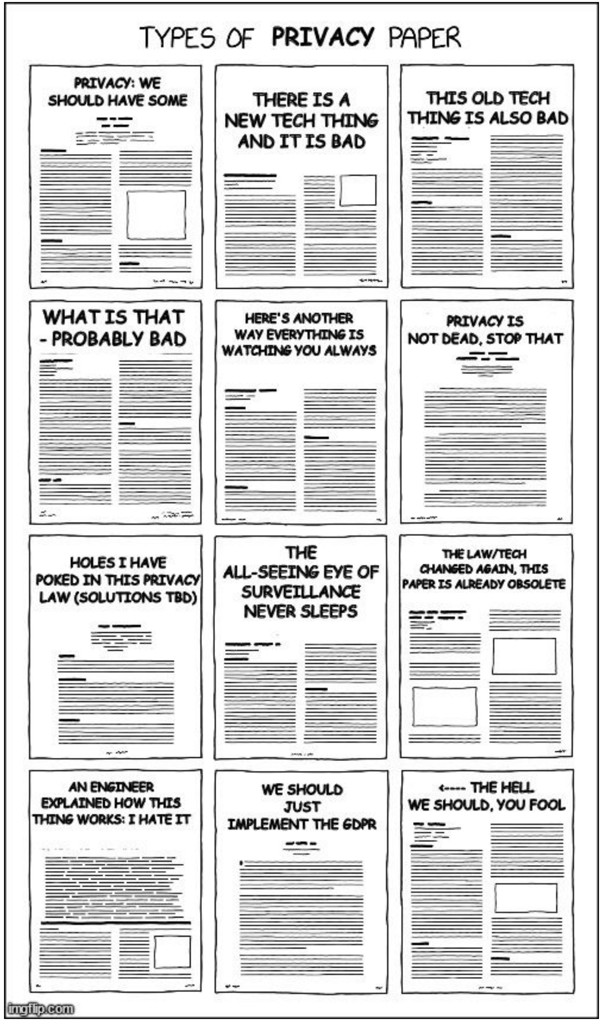
Your classmates >> a rubber duck

Ethics

- This guy (Andr Sellars) is going to visit and tell you more
- Absolutely no breaking of things without permission
  - Don't even look at things without permission
- Law is confusing - do not make assumptions
  - Ask for help if ever unsure


TYPES OF CYBERSECURITY PAPERS
I AM A CS PHD AND I HAVE DECIDED TO WRITE A PAPER ON SOCIOLOGY
A PROOF OF CONCEPT ATTACK THAT IS NEITHER PROOF NOR CONCEPT
A NOVEL AUTHENTICATION METHOD THAT IS IMPOSSIBLE TO DEPLOY
PLEASE TAKE THIS EXOTIC ATTACK CHAIN SERIOUSLY
CYBERSECURIT Y POLICY IS JUST LIKE MAD POLICY BUT THIS TIME I'M RIGHT
OUR IRB GAVE US A WAIVER FOR THIS LOL
WE SOLVED THIS PROBLEM WITH AI
<- NO THEY DID NOT
PRIVACY: WHAT EVEN IS IT? A COMPENDIUM
I HAD A GRAD STUDENT COUNT ALL THE MEAN POSTS ON THIS SOCIAL NETWORK AND BOY HOWDY THERE SURE ARE A LOT
A SERIOUS REGULATORY PROPOSAL COMPLETELY DIVORCED FROM TECHNICAL REALITY
IT WAS, IN FACT, DNS

Write up your results into a snazzy paper!


TYPES OF PRIVACY PAPER
PRIVACY: WE SHOULD HAVE SOME
THERE IS A NEW TECH THING AND IT IS BAD
THIS OLD TECH THING IS ALSO BAD
WHAT IS THAT - PROBABLY BAD
HERE'S ANOTHER WAY EVERYTHING IS WATCHING YOU ALWAYS
PRIVACY IS NOT DEAD, STOP THAT
HOLES I HAVE POKED IN THIS PRIVACY LAW (SOLUTIONS TBD)
THE ALL-SEEING EYE OF SURVEILLANCE NEVER SLEEPS
THE LAW/TECH CHANGED AGAIN, THIS PAPER IS ALREADY OBSOLETE
AN ENGINEER EXPLAINED HOW THIS THING WORKS: I HATE IT
WE SHOULD JUST IMPLEMENT THE GDPR
<---- THE HELL WE SHOULD, YOU FOOL
imgflip.com