Recitation 2: Choosing a Project Topic

6.5610 Applied Cryptography, Spring 2026

Jophy Ye Xiaochen Zhu
Adopted from slides by Kyle Hogan

February 13, 2026

Roadmap

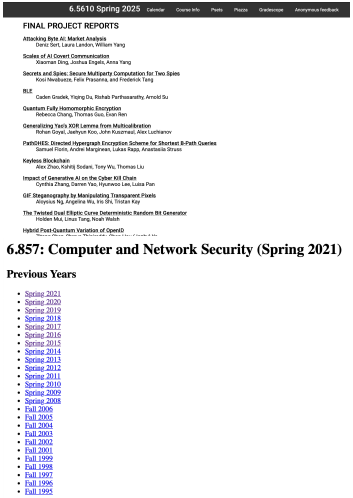
- Choosing and refining ideas
- Finding / reading academic papers
- Project scale and prior work
- Collaboration
- Please don't make us go to court
- Meet with staff next week

Choosing project ideas

- What do you love?
  - Hobbies? Your favorite class?
  - Security is everywhere
- What do you use?
  - Caller ID?
  - The unlock button on a car remote?
  - Homomorphic encryption?
  - Theoretical projects?
- 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 the result itself
  - Programming? Reverse engineering? Theory?

Choosing project ideas (cont.)

- We have an amazing repository of websites of this course dating back to 1995.
  - https://65610.csail.mit.edu/2026/past
- Past projects include *but not limited to*:
  - Red-teaming, implementation
  - Infrastructure, network security, hardware, etc.
  - Better schemes for "newer" topics in cryptography: multi-party computation, secret sharing, privacy-preserving systems, secure voting, blockchain, zero-knowledge proof, homomorphic or post-quantum encryption.
  - Machine learning $\times$ cryptography, steganography
  - Theory
  - *Don't be limited to this list!!!*



6.5610 Spring 2025 Calendar Course Info Piazza Piazza Gradescope Anonymous feedback

FINAL PROJECT REPORTS

Attacking Byte AI: Market Analysis
Deniz Sert, Laura Landon, William Yang

Scales of AI Covert Communication
Xiaoman Ding, Joshua Engels, Anna Yang

Secrets and Spies: Secure Multiparty Computation for Two Spies
Kosi Nwobodo, Felix Prasanna, and Frederick Tang

BLE
Caden Gradek, Yiqing Du, Rishab Parthasarathy, Arnold Su

Quantum Fully Homomorphic Encryption
Rebecca Chang, Thomas Guo, Evan Ren

Generalizing Yao's XOR Lemma from Multicalibration
Rohan Goyal, Jaehyun Koo, John Kuszmaul, Alex Lombardo

PathGHES: Directed Hypergraph Encryption Scheme for Shortest S-Path Queries
Samuel Florin, Andrei Margineni, Lukas Rapp, Anastasia Struzo

Keyless Blockchain
Alex Zhou, Kshitij Sodani, Tony Wu, Thomas Liu

Impact of Generative AI on the Cyber Kill Chain
Cynthia Zhang, Darren Yao, Hyunwoo Lee, Luisa Pan

GIF Steganography by Manipulating Transparent Pixels
Aliyyssa Ng, Angelina Wu, Iris Shi, Tristan Kay

The Twisted Dual Elliptic Curve Deterministic Random Bit Generator
Holden Mui, Linus Tang, Noah Walsh

Hybrid Post-Quantum Variation of OpenID

6.857: Computer and Network Security (Spring 2021)

Previous Years

- Spring 2021
- Spring 2020
- Spring 2019
- Spring 2018
- Spring 2017
- Spring 2016
- Spring 2015
- Spring 2014
- Spring 2013
- Spring 2012
- Spring 2011
- Spring 2010
- Spring 2009
- Spring 2008
- Fall 2006
- Fall 2005
- Fall 2004
- Fall 2003
- Fall 2002
- Fall 2001
- Fall 1999
- Fall 1998
- Fall 1997
- Fall 1996
- Fall 1995

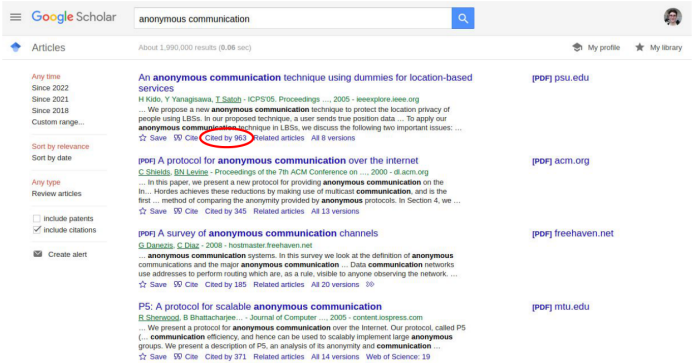
Refining your topic

- 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?

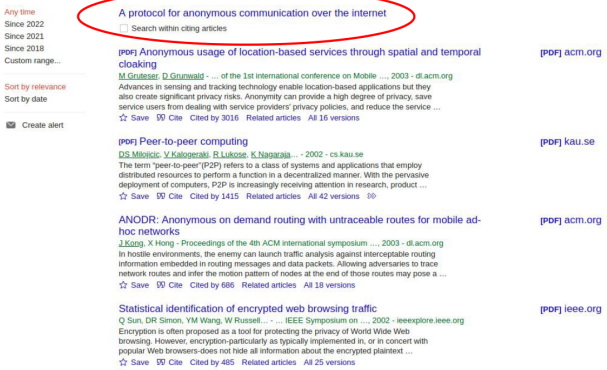
How to find papers

- Google Scholar: `scholar.google.com`
- Query example: *anonymous communication*
- Use "Cited by"
  - Generally corresponds to influence
  - Look at works citing a paper to find similar follow-up work

Google Scholar (example results)



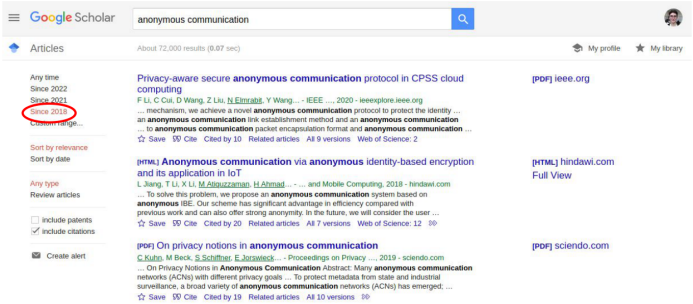
Google Scholar (citing articles)



How to find papers: year

- Old $\neq$ 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

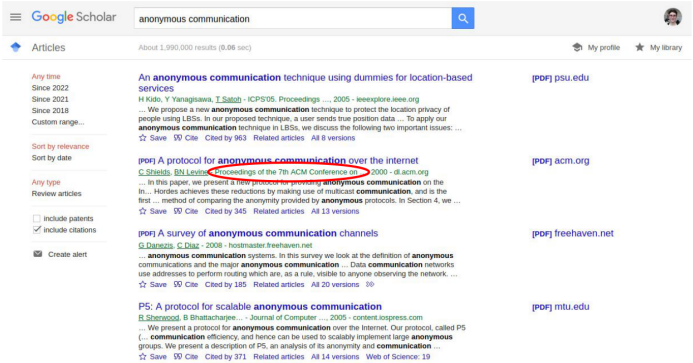
Google Scholar (recent papers)



How to find papers: conference tier

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

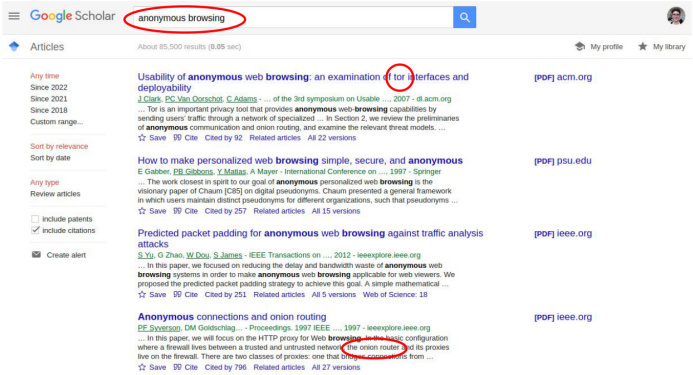
Google Scholar (more results)



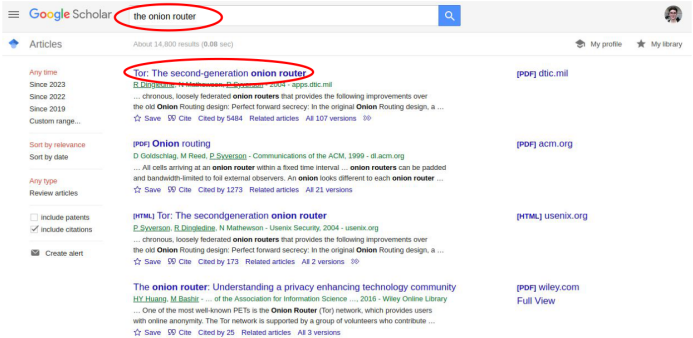
How to find papers: terminology

- 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 in my anonymous communication searches? (not there)

Google Scholar (anonymous browsing)



Google Scholar (the onion router)



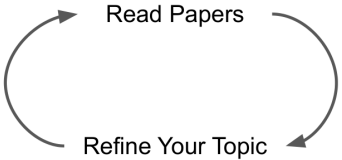
How to read papers

- Don't read the whole thing top-to-bottom as soon as you find it
- Read the abstract
  - Does it still seem relevant?
- Read the introduction
  - Summary of the paper's contributions + motivation
  - Does the paper still seem relevant?
- Read related works
  - Find other papers in the area (and why this paper thinks they didn't solve the problem)
  - Find papers that cite this paper in their related works to see what might have been missed
- Read the rest of the paper (optional)
  - Read full papers for works closely related to yours

Refining your topic (example)

- 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

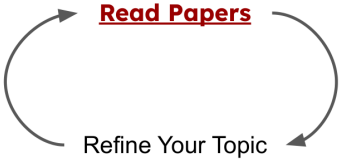
Read papers ↔ refine your topic



Roadblocks

- Novelty: 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: the problem is either "solved" or "unsolved" with no middle ground
  - You want steps along the way
  - Checkpoints should be meaningful in their own right
  - Move the goalposts
  - See: papers with titles like "Towards . . . "

Read papers ↔ refine your topic



Finding papers (redux)

- Cite related work
  - Important for your understanding of the topic
  - Credit where credit is due
- It's okay if you miss some papers initially
  - Or even over time (course staff can help)
  - Very important to do your best
  - Repeat your searches as your understanding grows

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 $\gg$ a rubber duck

Ethics

- Absolutely no breaking of things without permission
  - Don't even look at things without permission
- Go to the BU/MIT Student Innovations Law Clinic with legal questions
  - https://www.bu.edu/law/experiential-learning/clinics/bu-mit-student-innovations-law-clinic/
- Law is confusing — do not make assumptions
  - Ask for help if ever unsure
- Court order from MBTA to past students of this class:
  - https://thetech.com/2008/08/25/subway-v128-n31

Ethics (cont.)

- Bug bounties: some companies have a policy about security research involving them
- Responsible disclosure: if you find a problem you must let the organization know before you make it public

Upcoming deliverables

- Today: post preliminary project idea(s) on Piazza
  - One per person (even for full teams) in "Search for Teammates"
  - 4-5 sentences
  - Describe what the problem is, why it's important/interesting, and ideas for approach
  - Make/Join groups based on topic interest
- Project proposal
  - Officially due 2/20
  - Set up weekly meeting times with your group
  - Turn in:
    - a list of your team members
    - one or more tentative project ideas you all are excited about (one sentence is fine)
    - a weekly meeting time that all team members can make
    - a week-by-week timeline for the rest of the semester, with milestones each week