

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** × **cryptography**, steganography
 - Theory
 - *Don't be limited to this list!!!*

6.5610 Spring 2025 [Calendar](#) [Course Info](#) [Psets](#) [Papers](#) [Gradescope](#) [Anonymous Feedback](#)

FINAL PROJECT REPORTS

Attacking Byte AC Market Analysis
David Scott, Laura Lander, William Yang

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

Secrets and Spies: Secure Multiparty Computation for Two Spies
Koki Newsholtz, Felix Pflaum, and Frederik Tang

BLE
Caden Goodk, Yiting Di, Rishabh Parthasarathy, Arnold Gu

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

Generalizing Yao's XOR Lemma from Multicoalitions
Rohan Goyal, Jethyan Koo, John Kuszmaul, Alex Lombardi

PathHIDE: Directed Hypergraph Encryption Scheme for Shortest S-Path Queries
Samuel Flouri, Andre Margreth, Lukas Rupp, Anandesh Srinan

Keyless Blockchain
Alex Zhao, Kishij Sodani, Tony Wu, Thomas Lu

Impact of Generative AI on the Cyber Kill Chain
Qiyi Zhang, Daniel Yao, Hyeonwoo Lee, Lissa Pan

GF Steganography by Manipulating Translucent Pixels
Alyssa Ng, Angeline Wu, Ho Shi, Tristan Kay

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

Hybrid Post-Quantum Signature of OpenID
OpenID is a trademark of OpenID Foundation, Inc. All rights reserved.

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)

The screenshot shows the Google Scholar interface with the search term "anonymous communication". The search results are filtered to "Articles" and show approximately 1,990,000 results. The first result is "An anonymous communication technique using dummies for location-based services" by H Kido, Y Yanagisawa, and T Satoh, published in ICPS'05. The citation count "Cited by 963" is circled in red. Other results include a protocol for anonymous communication over the internet, a survey of anonymous communication channels, and a protocol for scalable anonymous communication.

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 [PDF] psu.edu
 H Kido, Y Yanagisawa, T Satoh - ICPS'05, Proceedings ..., 2005 - IEEE Xplore, 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] 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 Internet. Hordes achieves these reductions by making use of **anonymous 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] A survey of **anonymous communication** channels [PDF] freehaven.net
 C 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

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

Google Scholar (citing articles)

Any time
 Since 2022
 Since 2021
 Since 2018
 Custom range...

Sort by relevance
 Sort by date

Create alert

A protocol for anonymous communication over the internet

Search within citing articles

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

[PDF] Peer-to-peer computing
[DS Milošević](#), [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

[PDF] kau.se

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

[PDF] acm.org

Statistical identification of encrypted web browsing traffic
 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

[PDF] ieee.org

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)

The screenshot shows the Google Scholar interface with the search term "anonymous communication". The results are filtered to "Articles" and show approximately 72,000 results. The left sidebar contains filters for time range, sorting, and review options. The "Since 2019" filter is highlighted with a red circle. Three search results are visible, each with a title, authors, abstract snippet, and links for PDF, HTML, or Full View.

Google Scholar

anonymous communication

Articles About 72,000 results (0.07 sec) My profile My library

Any time
 Since 2022
 Since 2021
 Since 2019
 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 [PDF] ieeee.org
 F Li, C Cui, D Wang, Z Liu, H Elmehrik, 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** ...
 ☆ Save Cite Cited by 10 Related articles All 9 versions Web of Science: 2

[HTML] **Anonymous communication** via **anonymous** identity-based encryption and its application in IoT [HTML] hindawi.com
 L Jiang, T Li, X Li, M Alotaizaman, 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 Cite Cited by 20 Related articles All 7 versions Web of Science: 12

[PDF] On privacy notions in **anonymous communication** [PDF] sciendo.com
 C Kubo, M Beck, S Schiffer, E Jorsweck... - 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 Cite Cited by 19 Related articles All 10 versions

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)

The screenshot shows the Google Scholar search interface. The search bar contains 'anonymous communication' and shows 'About 1,990,000 results (0.06 sec)'. The left sidebar contains filters for 'Any time', 'Sort by relevance', 'Any type', and 'Create alert'. The main results area lists several articles, with the second article's title 'A protocol for anonymous communication over the internet' circled in red. The first article is 'An anonymous communication technique using dummies for location-based services' by H Kido, Y Yanagisawa, and T Satoh. The second article is 'A protocol for anonymous communication over the internet' by C Shields and BN Levine. The third article is 'A survey of anonymous communication channels' by G Danezis and C Diaz. The fourth article is 'P5: A protocol for scalable anonymous communication' by R Sherwood and B Bhattacharjee.

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)

The screenshot shows the Google Scholar search interface. The search bar contains the text "anonymous browsing", which is circled in red. Below the search bar, the results are listed under the heading "Articles" with a subtext "About 85,500 results (0.05 sec)". On the left side, there are filters for "Any time" (with options for "Since 2022", "Since 2021", "Since 2018", and "Custom range..."), "Sort by relevance" and "Sort by date", "Any type" (with "Review articles" selected), and checkboxes for "Include patents" (unchecked) and "Include citations" (checked). There is also a "Create alert" option. The main content area displays three search results:

- Usability of anonymous web browsing: an examination of tor interfaces and deployability** [PDF] acm.org. Authors: J. Clark, P.C. Van Oorschot, C. Adams. Abstract: "... Tor is an important privacy tool that provides anonymous web-browsing capabilities by sending users' traffic through a network of specialized ...".
- How to make personalized web browsing simple, secure, and anonymous** [PDF] psu.edu. Author: E Gabber. Abstract: "... 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 ...".
- Predicted packet padding for anonymous web browsing against traffic analysis attacks** [PDF] ieee.org. Authors: S. Yu, G. Zhao, W. Dou, S. James. Abstract: "... 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 ...".
- Anonymous connections and onion routing** [PDF] ieee.org. Authors: P.F. Syverson, D.M. Goldschlag. Abstract: "... 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 ...".

Google Scholar (the onion router)

The screenshot shows the Google Scholar search interface. The search bar contains the text "the onion router", which is circled in red. Below the search bar, the results are displayed in a list format. The first result is "Tor: The second-generation onion router" by P. Syverson and B. D. Gligoleto, published in DTIC in 2004. This title is also circled in red. The second result is "Onion routing" by D. Goldschlag and M. Reed, published in Communications of the ACM in 1999. The third result is "Tor: The secondgeneration onion router" by P. Syverson and B. D. Gligoleto, published in Usenix Security in 2004. The fourth result is "The onion router: Understanding a privacy enhancing technology community" by H. Y. Huang and M. Bashir, published in the Association for Information Science in 2016. The left sidebar contains filters for time range, sorting options, and citation preferences.

Google Scholar **the onion router**

Articles About 14,800 results (0.08 sec) My profile My library

Any time
Since 2023
Since 2022
Since 2019
Custom range...

Sort by relevance
Sort by date

Any type
Review articles

Include patents
 Include citations
 Create alert

Tor: The second-generation onion router [PDF] dtic.mil
P. Syverson, B. D. Gligoleto, N. Mathewson, P. Syverson - 2004 - apps.dtic.mil
... chronous, loosely federated **onion routers** that provides the following improvements over the old **Onion** Routing design: Perfect forward secrecy: In the original **Onion** Routing design, a ...
☆ Save Cited by 5484 Related articles All 107 versions

[PDF] Onion routing [PDF] acm.org
D Goldschlag, M Reed, P Syverson - Communications of the ACM, 1999 - dl.acm.org
... All cells arriving at an **onion router** within a fixed time interval ... **onion routers** can be padded and bandwidth-limited to foil external observers. An **onion** looks different to each **onion router** ...
☆ Save Cited by 1273 Related articles All 21 versions

[HTML] Tor: The secondgeneration onion router [HTML] usenix.org
P Syverson, B D Gligoleto, N Mathewson - Usenix Security, 2004 - usenix.org
... chronous, loosely federated **onion routers** that provides the following improvements over the old **Onion** Routing design: Perfect forward secrecy: In the original **Onion** Routing design, a ...
☆ Save Cited by 173 Related articles All 2 versions

The **onion router**: Understanding a privacy enhancing technology community [PDF] wiley.com
HY Huang, M Bashir - ... of the Association for Information Science ..., 2016 - Wiley Online Library
... One of the most well-known PETs is the **Onion Router** (Tor) network, which provides users with online anonymity. The Tor network is supported by a group of volunteers who contribute ...
☆ Save Cited by 25 Related articles All 3 versions

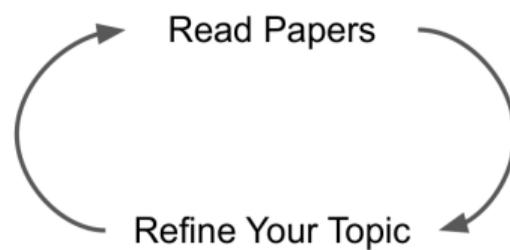
How to read papers

- 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 \leftrightarrow 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 \leftrightarrow 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