PAUL S. LOU

INTERESTS

Theoretical and applied cryptography: Public-key encryption, zero-knowledge proof systems, new hardness assumptions. Information theory. Quantum algorithms.

EDUCATION

'19-May '25 **Doctor of Philosophy in Computer Science**. University of California, Los Angeles (UCLA). Advised by Dr. Amit Sahai.

Dec. '18 University of Pennsylvania *Management & Technology* Dual Degree Program:

B.S.E. in Mathematics and Computer Science. School of Engineering and Applied Sciences.
Advised by Dr. Nadia Heninger.

B.S. in Economics, concentration in Statistics. The Wharton School.

RESEARCH EXPERIENCE

Sept. '25– **Bocconi University**. Postdoctoral Researcher *with Dr. Alon Rosen*.

Sept. – Dec. '23 **NTT Research**. Research Intern *with Dr. Abhishek Jain*.

Oct. '22 – Jan. '23 **Carnegie Mellon University**. Visiting Scholar *with Dr. Aayush Jain*.

May – Jun. '22 **Simons Institute for the Theory of Computing**. Visiting Graduate Student *for summer cluster: "Lattices and Beyond."*

May '16 – Dec. '18 **University of Pennsylvania**. Undergraduate Researcher *with Dr. Nadia Heninger*.

*All authors listed by alphabetical order, as is usual in cryptographic research.

PUBLICATIONS*

11. Quantum Advantage via Solving Multivariate Polynomials
Pierre Briaud, Itai Dinur, Riddhi Ghosal, Aayush Jain, Paul Lou, Amit Sahai.
SODA 2026
https://arxiv.org/abs/2509.07276

10. Fully Anonymous Secret Sharing
Allison Bishop, Matthew Green, Abhishek Jain, Yuval Ishai, Paul Lou.
Crypto 2025.
https://ia.cr/2025/1984

9. Post-Quantum PKE from Unstructured Noisy Linear Algebraic Assumptions: Beyond LWE and Alekhnovich's LPN
Riddhi Ghosal, Aayush Jain, Paul Lou, Amit Sahai, Neekon Vafa.
Eurocrypt 2025.
https://ia.cr/2025/844

8. Witness Semantic Security
Paul Lou, Nathan Manohar, Amit Sahai.

Eurocrypt 2024.
https://ia.cr/2024/1518

7. Computational Wiretap Coding from Indistinguishability Obfuscation
Yuval Ishai, Aayush Jain, Paul Lou, Amit Sahai, Mark Zhandry.
Crypto 2023.
https://ia.cr/2023/1270

6. Hard Languages in NP ∩ coNP and NIZK Proofs from Unstructured Hardness
Riddhi Ghosal, Yuval Ishai, Alexis Korb, Eyal Kushilevitz, Paul Lou, Amit Sahai.
STOC 2023.
https://dl.acm.org/doi/10.1145/3564246.3585119

5. Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum $i\mathcal{O}$
Aayush Jain, Rachel Lin, Paul Lou, Amit Sahai.
Eurocrypt 2023.
https://ia.cr/2022/1637

4. Efficient NIZKs from LWE via Polynomial Reconstruction and "MPC in the Head"
Riddhi Ghosal, Paul Lou, Amit Sahai.
Asiacrypt 2022.
https://ia.cr/2022/370

3. Beyond the Csiszár-Korner Bound: Best-Possible Wiretap Coding via Obfuscation
Yuval Ishai, Alexis Korb, Paul Lou, Amit Sahai.
Crypto 2022. Invited & accepted submission to *The Journal of Cryptology*.
https://ia.cr/2022/343

2. Relinearization Attack on LPN over Large Fields
Paul Lou, Amit Sahai, Varun Sivashankar.
CFAIL 2022 (Affiliated workshop at Crypto 2022). Invited & accepted submission to a special edition of *The Computer Journal*.
https://doi.org/10.1093/comjnl/bxad070

1. Post-quantum RSA
Daniel J. Bernstein, Nadia Heninger, Paul Lou, Luke Valenta
PQCRYPTO 2017
ia.cr/2017/351

PREPRINTS

2. A Note on the Pseudorandomness of Low-Degree Polynomials over the Integers
Aayush Jain, Alexis Korb, Paul Lou, Amit Sahai
https://ia.cr/2021/1415

1. Expanding COVID-19 Symptom Screening to Retail, Restaurants, and Schools by Preserving Privacy Using Relaxed Digital Signatures
   Brandon Jew, Alexis Korb, Paul Lou, Jeffrey N. Chiang, Ulzee An, Amit Sahai, Eran Halperin, Eleazar Eskin
   https://www.medrxiv.org/content/10.1101/2020.08.06.20169839v2

TEACHING & SERVICE

Reviewer for *Journal of Cryptology*. Reviewer for *Designs, Codes and Cryptography*. External reviewer for Crypto '22, '25, TCC '23, '24, '25, Eurocrypt '24, '25, STOC '24, '25, '26. Program committee (PC) member for Oakland 2023 Posters Program.

Co-lead instructor for CS-289: Advanced Topics in Cryptography (Quantum Cryptography), Spring 2023, UCLA.

Teaching assistant for

- CS-181: Formal Languages and Automata Theory, Winter 2021, Winter 2022, Winter 2024, UCLA.
- CIS-556: Cryptography (Graduate-level), Fall 2018, UPenn.
- CIS-548: Operating Systems (Graduate-level) Spring 2018, UPenn.
- CIS-380: Operating Systems, Fall 2017, Fall 2018 (Head TA), UPenn
- CIS-262: Theory of computation: Automata, Computability, & Complexity, Fall 2016, UPenn.

PROGRAMMING LANGUAGES

Preferred — Python, C++

Comfortable — OCaml, C, Java, Sage, Magma

PERSONAL INFORMATION

Languages

English · Mothertongue
Mandarin · Bilingual
French · B2
German · B1
Italian · A1

Nationality — US Citizenship

Email — pslou@cs.ucla.edu

Misc. Interests — Skiing · Swimming · Hot Chocolate

November 16, 2025