

Paul S. Lou

Postdoctoral Researcher | Bocconi University

paul.lou@unibocconi.it | paullou.me | Google Scholar | GitHub

INTERESTS

AI safety; LLM reasoning; inference; theoretical and applied cryptography: public-key encryption, zero-knowledge proof systems, new hardness assumptions; information theory; quantum algorithms.

RESEARCH EXPERIENCE

Bocconi University Postdoctoral Researcher with Dr. Alon Rosen.	Sep. 2025–present
NTT Research Research Intern with Dr. Abhishek Jain.	Sep.–Dec. 2023
Carnegie Mellon University Visiting Scholar with Dr. Aayush Jain.	Oct. 2022–Jan. 2023
Simons Institute for the Theory of Computing Visiting Graduate Student for summer cluster: “Lattices and Beyond.”	May–Jun. 2022
University of Pennsylvania Undergraduate Researcher with Dr. Nadia Heninger.	May 2016–Dec. 2018

EDUCATION

University of California, Los Angeles Doctor of Philosophy in Computer Science. Advised by Dr. Amit Sahai.	2019–May 2025
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.	Dec. 2018

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

IN SUBMISSION*

- S3 **Worst-Case Hardness for Succinct and Decomposed Learning with Errors**
Damiano Abram, Gal Arnon, Valerio Cini, **Paul Lou**, Giulio Malavolta, Lawrence Roy.
2026 | <https://eprint.iacr.org/2026/2443>
Subsumes Decomposed LWE is Equivalent to Succinct LWE.
- S2 **Limitations on Autoregressive Token Generation via Sequential Sampling**
Gal Arnon, Andrej Bogdanov, **Paul Lou**, Giulio Malavolta, Alon Rosen, Lorenzo Taschin.
2026 | <https://arxiv.org/abs/2610.14615>
- S1 **Post-Quantum PKE and More from a Noisy Unstructured Linear Algebraic Assumption: Beyond LWE and LPN**
Riddhi Ghosal, **Paul Lou**, Amit Sahai.
2026 | <https://eprint.iacr.org/2026/2113>

PUBLICATIONS*

- P12 **Expanders Meet Reed–Muller: Easy Instances of Noisy k -XOR**
Jarosław Błasiok, **Paul Lou**, Alon Rosen, Madhu Sudan.
FOCS 2026 [CORE A*] | <https://arxiv.org/abs/2604.04188>

- P11 **Quantum Advantage via Solving Multivariate Polynomials**
Pierre Briaud, Itai Dinur, Riddhi Ghosal, Aayush Jain, **Paul Lou**, Amit Sahai.
SODA 2026 [CORE A*] | <https://arxiv.org/abs/2509.07276>
- P10 **Fully Anonymous Secret Sharing**
Allison Bishop, Matthew Green, Yuval Ishai, Abhishek Jain, **Paul Lou**.
Crypto 2025 [CORE A*] | <https://eprint.iacr.org/2025/1984>
- P9 **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 [CORE A*] | <https://eprint.iacr.org/2025/844>
- P8 **Witness Semantic Security**
Paul Lou, Nathan Manohar, Amit Sahai.
Eurocrypt 2024 [CORE A*] | <https://eprint.iacr.org/2024/1518>
- P7 **Computational Wiretap Coding from Indistinguishability Obfuscation**
Yuval Ishai, Aayush Jain, **Paul Lou**, Amit Sahai, Mark Zhandry.
Crypto 2023 [CORE A*] | <https://eprint.iacr.org/2023/1270>
- P6 **Hard Languages in $NP \cap coNP$ and NIZK Proofs from Unstructured Hardness**
Riddhi Ghosal, Yuval Ishai, Alexis Korb, Eyal Kushilevitz, **Paul Lou**, Amit Sahai.
STOC 2023 [CORE A*] | <https://dl.acm.org/doi/10.1145/3564246.3585119>
- P5 **Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum iO**
Aayush Jain, Rachel Lin, **Paul Lou**, Amit Sahai.
Eurocrypt 2023 [CORE A*] | <https://eprint.iacr.org/2022/1637>
- P4 **Efficient NIZKs from LWE via Polynomial Reconstruction and "MPC in the Head"**
Riddhi Ghosal, **Paul Lou**, Amit Sahai.
Asiacrypt 2022 [CORE A] | <https://eprint.iacr.org/2022/370>
- P3 **Beyond the Csiszár-Korner Bound: Best-Possible Wiretap Coding via Obfuscation**
Yuval Ishai, Alexis Korb, **Paul Lou**, Amit Sahai.
Crypto 2022 [CORE A*] | <https://eprint.iacr.org/2022/343>
Invited and accepted submission to *Journal of Cryptology*.
- P2 **Relinearization Attack on LPN over Large Fields**
Paul Lou, Amit Sahai, Varun Sivashankar.
CFAIL 2022 [CORE: not listed] | <https://doi.org/10.1093/comjnl/bxad070>
Crypto-affiliated workshop. Invited and accepted submission to a special edition of *The Computer Journal*.
- P1 **Post-quantum RSA**
Daniel J. Bernstein, Nadia Heninger, **Paul Lou**, Luke Valenta.
PQCrypto 2017 [CORE C] | <https://eprint.iacr.org/2017/351>

PREPRINTS

- W2 **A Note on the Pseudorandomness of Low-Degree Polynomials over the Integers**
Aayush Jain, Alexis Korb, **Paul Lou**, Amit Sahai.
2021 | <https://eprint.iacr.org/2021/1415>
- W1 **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.
2020 | <https://www.medrxiv.org/content/10.1101/2020.08.06.20169839v2>

TALKS

- Limitations on Autoregressive Token Generation via Sequential Sampling
Bocconi seminar, Oct. 2026
- Quantum Advantage via Solving Multivariate Polynomials
University of Texas, Austin, Dec. 2025

- Fully Anonymous Secret Sharing
Crypto 2025
Stanford, Sep. 2025
- Ph.D. Thesis Defense
University of California, Los Angeles, May 2025
- Witness Semantic Security
Eurocrypt 2024
- Computational Wiretap Coding from Indistinguishability Obfuscation
Simons Institute Summer 2025
Conference on Information-Theoretic Cryptography 2024
Crypto 2023
- Hard Languages in $\text{NP} \cap \text{coNP}$ and NIZK Proofs from Unstructured Hardness
Carnegie Mellon University, Apr. 2024
- Beyond the Csiszár-Korner Bound: Best-Possible Wiretap Coding via Obfuscation
University of California, Los Angeles, Oral Qualifying Exam, Nov. 2023
- Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum iO
Eurocrypt 2023
- Efficient NIZKs from LWE via Polynomial Reconstruction and “MPC in the Head”
Asiacrypt 2022
- Relinearization Attack on LPN over Large Fields
CFAIL 2022

ACADEMIC SERVICE

Program committee (PC) member for Asiacrypt 2026, CCS 2026, Oakland 2023 Posters Program.

Reviewer for Journal of Cryptology and Designs, Codes and Cryptography.

External reviewer for Crypto ('22, '25, '26), Eurocrypt ('24, '25, '26), STOC ('24, '25, '26), FOCS ('26), TCC ('23, '24, '25), IEEE S&P ('24), Asiacrypt ('24), ITCS ('27), ICLR ('27).

TEACHING

Instructor

(Co-lead Instructor) CS-289: Advanced Topics in Cryptography (Quantum Cryptography), Spring 2023, University of California, Los Angeles.

Teaching assistant

CS-181: Formal Languages and Automata Theory, Winter 2021, Winter 2022, Winter 2024, University of California, Los Angeles.

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.

Mentorship

Varun Sivashankar (UCLA Undergraduate) → Princeton Ph.D. in Applied Mathematics.

PROGRAMMING LANGUAGES

<i>Preferred</i>	Python, C, C++
<i>Experienced</i>	OCaml, Java, Sage, Magma

PERSONAL INFORMATION

<i>Languages</i>	English (Mothertongue); Mandarin (Bilingual); French (B2); German (B1); Italian (B1).
<i>Nationality</i>	US Citizenship
<i>Email</i>	paul.lou@unibocconi.it
<i>Misc. Interests</i>	Skiing · Swimming · Hot Chocolate