PAUL S. LOU

INTERESTS

Theoretical and applied cryptography, information theory

EDUCATION

2019-Present **Ph.D. Candidate** at UCLA advised by Prof. Amit Sahai.
Masters in Computer Science, UCLA (June 2021).

Dec. 2018 University of Pennsylvania *Management & Technology* dual degree program:

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

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

PREPRINTS

1. 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

PUBLICATIONS

All authors listed by alphabetical order.

7. Computational Wiretap Coding from Indistinguishability Obfuscation
   Yuval Ishai, Aayush Jain, Paul Lou, Amit Sahai, Mark Zhandry.
   CRYPTO 2023.
   To appear.

6. Hard Languages in $\mathsf{NP} \cap \mathsf{coNP}$ and NIZK Proofs from Unstructured Hardness
   Riddhi Ghosal, Yuval Ishai, Alexis Korb, Eyal Kushilevitz, Paul Lou, Amit Sahai.
   STOC 2023.
   To appear.

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 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. Invited submission to a special edition of *The Computer Journal*.
https://tinyurl.com/23a274dd

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

TEACHING & SERVICE

Reviewer for Journal of Cryptology. External reviewer for CRYPTO 2022, TCC 2023. Program committee (PC) member for Oakland 2023 Posters Program.

Co-lead 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, 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

PERSONAL INFORMATION

Languages — English · Mothertongue
Mandarin · Bilingual
French · B1

Nationality — US Citizenship

Email — pslou@cs.ucla.edu

Misc. Interests — Skiing · Climbing · Hot Chocolate

June 12, 2023