

PAUL S. LOU

INTERESTS

Theoretical and applied cryptography, information theory, quantum computation

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

- In-submission* 1. Polynomial-Time Cryptanalysis of the Subspace Flooding Assumption for Post-Quantum $i\mathcal{O}$
Aayush Jain, Rachel Lin, Paul Lou, Amit Sahai
- In-submission* 2. Efficient NIZKs from LWE via Polynomial Reconstruction and “MPC in the Head”
Riddhi Ghosal, Paul Lou, Amit Sahai
<https://ia.cr/2022/370>
- In-submission* 3. Beyond the Csiszár-Korner Bound: Best-Possible Wiretap Coding via Obfuscation
Yuval Ishai, Alexis Korb, Paul Lou, Amit Sahai
<https://ia.cr/2022/343>
4. 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

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

SERVICE

External reviewer for CRYPTO 2022.

TEACHING

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.

COMPUTER LANGUAGES

<i>Preferred</i>	PYTHON, C++
<i>Comfortable</i>	OCAML, C, JAVA

PERSONAL INFORMATION

<i>Languages</i>	ENGLISH · Mothertongue
	MANDARIN · Bilingual
	FRENCH · B1
<i>Nationality</i>	US Citizenship
<i>Email</i>	pslou@cs.ucla.edu
<i>Misc. Interests</i>	Skiing · Climbing · Hot Chocolate

March 31, 2022