Yixin Shen

Postdoctoral researcher at Royal Holloway University of London

Flat 6, Tudor Court, Church Road
Egham, Surrey
TW20 9HZ, UK
+447448509760
yixin.shen@rhul.ac.uk
www.irif.fr/~yixin.shen/
Date of birth: 07/24/1992
French citizenship

Education

10/2017–05/2021 **PhD in Computer Science**, *Université de Paris*, France, Classical and Quantum Cryptanalysis for Euclidean Lattices and Subset Sums, Supervised by Frédéric Magniez.
- 12/2017–06/2018 : 6-month research internship with TEAM Erasmus Mundus scholarship at Japanese-French Laboratory for Informatics (JFLI) and the University of Tokyo, supervised by Phong Q. Nguyen
- 07/2019-08/2019 : 2-month research internship at Center for Quantum Technologies (CQT) at the National University of Singapore, supervised by Divesh Aggawal

2016–2017 **Parisian Master of Research in Computer Science (MPRI)**, *Université de Paris*.
Master in Computer Science. Major in Cryptology (with honor).

2016–2017 **Télécom Paris**, *Paris*, France.
An engineering degree program (Master's degree) to complete the study in Ecole Polytechnique. Major in Computer Science.

2013–2017 **École Polytechnique**, *Palaiseau*, France.
A 4-year engineering degree program (Bachelor's+Master's degree) in one of France's most prominent institutions of science and engineering (Grandes Ecoles). Major in Mathematics and in Computer Science.

Work Experience

03/2021–present **Postdoctoral researcher**, *Royal Holloway University of London*, UK.
Hosted by Professor Martin R. Albrecht

2017– 2020 **Teaching assistant**, *Université de Paris*, France.
- Introduction to Java programming (24 hours tutorial $\times 3$)
- Object-oriented programming and graphical user interface (36 hours tutorial $\times 2$)
- Advanced Object-oriented programming (36 hours tutorial)

02/2017–08/2017 **Research internship**, *Orange R&D*, Châtillon, France.
- Topic : designing a white-box AES
- Supervisor : Gilles Macario-Rat
- Candidate implementation in C++ and participation in the CHES 2017 Whitebox Contest

03/2016–07/2016 **Research internship**, *Japanese-French Laboratory for Informatics (JFLI) and the University of Tokyo*, Japan.
- Topic : Bleichenbacher's method for solving the Hidden Number Problem (HNP)
- Supervisor : Phong Q. Nguyen
- Research Prize of Ecole Polytechnique

06/2015–08/2015 **Engineering Internship**, *EDF R&D (Electricity of France)*, Clamart, France.
Studied the applicability of existing methods used by Intrusion Detection Systems (IDS) to industrial networks (especially Artificial Neural Networks). Implementation in Python.

09/2014–06/2015 **Teaching Assistant**, *Lycée Louis-le-Grand*, Paris, France.
Training of a group of 3 students in Mathematics in order to prepare them for the "Grandes Ecoles" competitive exams (1h / week)

09/2013–03/2014 **Social work Internship**, *Apprentis d'Auteuil*, Saint-Maurice-Saint-Germain, France.
Training and teaching young students in scholar and social difficulties to help them re-integrate the educational system.

Research Publications

2022 **Variational quantum solutions to the Shortest Vector Problem**, *Preprint*, Martin R. Albrecht, Miloš Prokop, Yixin Shen, Petros Wallden.

2022 **Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *Preprint, extended version of STACS 2021*, Accepted as a contributed talk at QIP 2022, Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Yixin Shen.

2021 **Improved (Provable) Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *STACS 2021*, Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Yixin Shen.

2021 **Fast Classical and Quantum Algorithms for Online k-server Problem on Trees**, *ICTCS 2021*, Ruslan Kapralov, Kamil Khadiev, Joshua Mokut, Yixin Shen, Maxim Yagafarov.

2020 **Improved Classical and Quantum Algorithms for Subset-Sum**, *ASIACRYPT 2020*, Xavier Bonnetain, Rémi Bricout, André Schrottenloher, Yixin Shen .

2020 **Quantum Lower and Upper Bounds for 2D-Grid and Dyck Language**, *MFCS 2020*, Andris Ambainis, Kaspars Balodis, Janis Iraids, Kamil Khadiev, Vladislavs Klevickis, Krisjanis Prusis, Yixin Shen, Juris Smotrovs, Jevgenijs Vihrovs .

2018 **Quantum Lattice Enumeration and Tweaking Discrete Pruning**, *ASIACRYPT 2018*, Yoshinori Aono, Phong Q. Nguyen, Yixin Shen .

Talks

2022 **Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *GT info-quantique LaBRI*.

2021 **Provable quantum algorithms for SVP**, *Dagstuhl Seminar 21421 Quantum Cryptanalysis*.

2021 **Improved (Provable) Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *Royal Holloway Information Security Group Seminar 2021*.

2020 **Improved Classical and Quantum Algorithms for Subset-Sum**, *Joint Inria-IRIF Seminar 2020, Chinese Academy of Sciences 2020, Asiacrypt 2020, Journées Codage & Cryptographie 2020*.

2018, 2019 **Quantum Lattice Enumeration and Treaking Discrete Pruning**, *Asiacrypt 2018, Journées Informatique Quantique 2018, Journées Codage & Cryptographie 2018, EQTC 2019*.

2018, 2019 **The shortest vector problem : Classical and Quantum Approaches**, *CQIS, University of Technology Sydney 2018, ATOS 2019*.

Services

I have been a reviewer for : TQC 2019, ANTS 2020, SODA 2021, ICALP 2021, CRYPTO 2021, ASIACRYPT 2021, SAC 2021. I am in charge of organizing the ENSL/CWI/RHUL Joint Online Cryptography seminars.

Languages

Chinese	Native, Mandarin & Shanghainese	French	Fluent
English	Advanced	Japanese	Lower intermediate

Programming Languages and Tools

Java, Python, C++, OCaml, SageMath, LaTex

Hobbies

Badmintion : ranked ~4000/30000 in France. Elected member of the executive committee of CPS10 badminton club in Paris (~400 members). Tennis : playing league matches for Ashford Tennis Club. Hiking. Traveling (37 countries). Going to art exhibitions.