Yixin Shen

Research Fellow 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

Research Interests

I work broadly across the fields of cryptography and quantum algorithms. My research interests are centered on quantum algorithms applied to lattice-based cryptography. I have made several contributions to state-of-the-art classical and quantum attacks on key problems for post-quantum cryptography. I am also interested in broader topics such as theoretical computer science or computational complexity.

Work Experience

08/2022– present **Research Fellow**, *Royal Holloway University of London*, UK
Principal investigator of UKRI grant EP/W02778X/1 (5 years, £585,075)

03/2021– 07/2022 **Postdoctoral researcher**, *Royal Holloway University of London*, UK
Hosted by Professor Martin R. Albrecht

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

07/2019– 08/2019 **Research Internship**, *Center for Quantum Technologies (CQT)* , National University of Singapore
Supervisor : Divesh Aggawal

12/2017– 06/2018 **Research Internship**, *Japanese-French Laboratory for Informatics (JFLI)*, University of Tokyo
TEAM Erasmus Mundus scholarship, Supervisor : Phong Q. Nugyen

02/2017– 08/2017 **Research internship**, *Orange R&D*, Châtillon, France
Supervisor : Gilles Macario-Rat

03/2016– 07/2016 **Research internship**, *Japanese-French Laboratory for Informatics (JFLI)*, University of Tokyo
Research Prize of Ecole Polytechnique, Supervisor : Phong Q. Nguyen

06/2015– 08/2015 **Engineering Internship**, *EDF R&D (Electricity of France)*, Clamart, France
Studied the applicability of Intrusion Detection Systems (IDS) to industrial networks.

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

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

Education

10/2017– 05/2021 **PhD in Computer Science**, *Université de Paris Cité*, France, Classical and Quantum Cryptanalysis for Euclidean Lattices and Subset Sums, Supervised by Frédéric Magniez

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.

2016–2017 **Parisian Master of Research in Computer Science (MPRI)**, *Université de Paris Cité* , France
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.

Research Publications

2022 **Faster Dual Lattice Attacks by Using Coding Theory**, *In submission*, Kevin Carrier, Yixin Shen, Jean-Pierre Tillich

2022 **Quantum Augmented Dual Attack**, *In submission*, Martin R. Albrecht, Yixin Shen

2022 **Finding many Collisions via Reusable Quantum Walks**, *In submission*, Xavier Bonnetain, André Chailloux, André Schrottenloher, Yixin Shen

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

2022 **Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *Contributed talk at QIP 2022*, Extended version of STACS 2021 with major differences, 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 **Faster Dual Lattice Attacks by Using Coding Theory**, *GT codes-crypto Inria Paris*

2022 **Quantum Augmented Dual Attack**, *NIST 4th PQC Workshop, Bristol Quantum Cryptanalysis Workshop*

2022 **Finding many Collisions via Reusable Quantum Walks**, *IRIF Seminar, Bristol QIT Seminar*

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

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 ISG Seminar*

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

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

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

Grant

I am the principal investigator of UKRI grant EP/W02778X/1 (2022-2027, £585,075).

Services

Conference reviewer : TQC 2019, ANTS 2020, SODA 2021, ICALP 2021, CRYPTO 2021, ASIACRYPT 2021, SAC 2021, TCC 2022, ASIACRYPT 2022, SODA 2022, PKC 2022.
Journal reviewer : ACM Transaction on Quantum Computing, Designs Codes and Cryptography.
Seminar organizer : ENSL/CWI/RHUL Joint Online Cryptography seminars.
PC member : INDOCRYPT 2022.

Member of the EPSRC Peer Review College.

Languages

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

Programming Languages and Tools

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