

Yixin Shen

Full-time Researcher at Inria Rennes

54 Boulevard Raymond Poincaré
35700, Rennes, France
☎ +33620572641
✉ yixin.shen@inria.fr
🌐 <https://yixinshen.github.io>
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

- 07/2024– **Full-time Researcher (Chargée de Recherche)**, *Inria Rennes, Team CAPSULE, France*
- 08/2023– **Research Fellow**, *King's College London, UK*
 - 06/2024 Principal investigator of UKRI grant EP/W02778X/1 (£585,075)
- 03/2021– **Postdoctoral Researcher then Research Fellow**, *Royal Holloway University of London, UK*
 - 08/2023 Hosted by Professor Martin R. Albrecht
- 2017– 2020 **Teaching assistant**, *Université Paris Cité, France*
 - Introduction to Java programming (tutorials, 24 hours × 3 years)
 - Object-oriented programming and graphical user interface (tutorials, 36 hours × 2 years)
 - Advanced Object-oriented programming (tutorials, 36 hours)
- 07/2019– **Research Internship**, *Center for Quantum Technologies (CQT)*, National University of Singapore
 - 08/2019 Supervisor : Divesh Aggarwal
- 12/2017– **Research Internship**, *Japanese-French Laboratory for Informatics (JFLI)*, University of Tokyo
 - 06/2018 TEAM Erasmus Mundus scholarship, Supervisor : Phong Q. Nguyen
- 02/2017– **Research Internship**, *Orange R&D, Châtillon, France*
 - 08/2017 Supervisor : Gilles Macario-Rat
- 03/2016– **Research internship**, *Japanese-French Laboratory for Informatics (JFLI)*, University of Tokyo
 - 07/2016 Research Prize of Ecole Polytechnique, Supervisor : Phong Q. Nguyen
- 06/2015– **Engineering Internship**, *EDF R&D (Electricity of France)*, Clamart, France
 - 08/2015 Studied the applicability of Intrusion Detection Systems (IDS) to industrial networks.
- 09/2014– **Teaching Assistant**, *Lycée Louis-le-Grand, Paris, France*
 - 06/2015 Training of a group of 3 students in Mathematics for the “Grandes Ecoles” competitive exams (1h/week)
- 09/2013– **Social work Internship**, *Apprentis d'Auteuil, Saint-Maurice-Saint-Germain, France*
 - 03/2014 Training young students in scholar and social difficulties to help them re-integrate the educational system.

Education

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

- 2025 **Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *SIAM Journal on Computing* 2025, Divesh Aggarwal, Yanlin Chen, Rajendra Kumar, Yixin Shen
- 2025 **Discrete gaussian sampling for BKZ-reduced basis**, *ArcticCrypt* 2025, Amaury Pouly, Yixin Shen
- 2024 **Does quantum lattice sieving require quantum RAM**, *Preprint* 2024, Beomgeun Cho, Minki Hhan, Taehyun Kim, Jeonghoon Lee, Yixin Shen
- 2024 **Smoothing Parameter and Shortest Vector Problem on Random Lattices**, *Preprint* 2024, Amaury Pouly, Yixin Shen
- 2024 **Provable Dual Attacks on Learning with Errors**, *EUROCRYPT* 2024, Amaury Pouly, Yixin Shen
- 2023 **Quantum bounds for 2D-grid and Dyck language**, *QUANTUM INFORMATION PROCESSING* 2023, Andris Ambainis, Kaspars Balodis, Janis Iraids, Kamil Khadiev, Vladislavs Klevickis, Krisjanis Prusis, Yixin Shen, Juris Smotrovs, Jevgenijs Vihrovs
- 2023 **Finding many Collisions via Reusable Quantum Walks**, *EUROCRYPT* 2023, Xavier Bonnetain, André Chailloux, André Schrottenloher, Yixin Shen
- 2023 **Variational quantum solutions to the Shortest Vector Problem**, *QUANTUM* 7, 2023, Martin R. Albrecht, Miloš Prokop, Yixin Shen, Petros Wallden
- 2022 **Faster Dual Lattice Attacks by Using Coding Theory**, *Preprint*, Kevin Carrier, Yixin Shen, Jean-Pierre Tillich
- 2022 **Quantum Augmented Dual Attack**, *NIST 4th PQC Standardization Conference* 2022, Martin R. Albrecht, Yixin Shen
- 2022 **Improved Classical and Quantum Algorithms for the Shortest Vector Problem via Bounded Distance Decoding**, *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 Moku, 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

Scientific Talks

- 2023 **Tutorial : Quantum Algorithms for Lattice Problems**, *Dagstuhl Seminar 23421 Quantum Cryptanalysis*, *Shonan Seminar 198 New Directions in Provable Quantum Advantages*, *Academia Sinica Taiwan*
- 2023 **On Dual Attacks against the Learning With Errors Problem**, *Séminaire Caramba Université de Nancy*, *Séminaire de Cryptographie Université de Rennes 1*
- 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, 2023 **Finding many Collisions via Reusable Quantum Walks**, Séminaire IRIF Université Paris Cité, Bristol QIT Seminar, Quantum Software Lab Workshop University of Edinburgh, London-ish Lattice Coding & Crypto Meeting Imperial College London, UK Crypto Day King's College London, ANR QuDATA Workshop Bordeaux
- 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**, ISG Seminar Royal Holloway University of London
- 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 Treating Discrete Pruning**, Asiacrypt, Journées Informatique Quantique, Journées Codage & Cryptographie, European Quantum Technology Conference
- 2018, 2019 **The shortest vector problem : Classical and Quantum Approaches**, CQIS Seminar University of Technology Sydney, ATOS

Grant

I am the principal investigator of UKRI grant [EP/W02778X/1](#) (£585,075), awarded as Quantum Technology Career Development Fellowship.

Services

- Program committee member : INDOCRYPT 2022, 2023, 2024.
- Conference reviewer : TQC 2019, ANTS 2020, SODA 2021, ICALP 2021, CRYPTO 2021, ASIACRYPT 2021, SAC 2021, TCC 2022, ASIACRYPT 2022, SODA 2022, PKC 2022, CRYPTO 2023, ASIACRYPT 2023, EUROCRYPT 2024, CRYPTO 2024, INSCRYPT 2024, EUROCRYPT 2025, PKC 2025.
- Journal reviewer : ACM Transaction on Quantum Computing, Designs Codes and Cryptography, Quantum Journal, SIAM Journal on Applied Algebra and Geometry.
- Seminar organizer : ENSL/CWI/KCL Joint Online Cryptography seminars.
- Conference/Workshop local organizer : QUANTALGO Workshop 2018, ICALP 2022.
- PhD thesis external examiner : Edmund Dable-Heath (Imperial College London), Clément Ducros (Université Paris Cité)
- Member of the EPSRC Peer Review College.

Media Outreach

Panelist at the Responsible Quantum Summit organised by Tortoise Media :
 "What are the implications of advancements in quantum technology for the security ?"

Languages

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

Programming Languages and Tools

Java, Python, C++, OCaml, SageMath, LaTeX