Mina Doosti

Curriculum Vitae

Informatics Forum, 10 Crichton St, Edinburgh EH8 9AB, UK
✉ *mdoosti@ed.ac.uk*

Overview

I am a Chancellor's Fellow (UK equivalent of tenure-track assistant professor) at the University of Edinburgh. As a researcher in quantum information sciences and cryptography, my focus is on the intersection of quantum computing with cryptography and learning theory. I aim to bridge different disciplines in computer science, physics, and mathematics to tackle theoretical problems, identify bottlenecks in current quantum architectures, and develop novel applications for quantum technologies.

Education

2018–2022 **PhD**, Doctor of Philosophy from *The Laboratory for Foundations of Computer Science (LFCS), School of Informatics, University of Edinburgh*
Thesis title: Unclonability and Quantum Cryptanalysis: From Foundations to Applications.
Supervisor: Prof.Elham Kashefi, Second Supervisor: Dr. Myrto Arapinis
Examiners: Anne Broadbent and Petros Wallden

2015–2017 **M.Sc. in Physics**, *Physics Department, Sharif University of Technology*
Thesis title: Superposition of orthogonal states and no-go theorems in Quantum Mechanics.
Supervisor: Prof. Vahid Karimipour

2010–2014 **B.Sc. in Physics**, *Physics Department, Sharif University of Technology*.

Research Experience

2023-now **Chancellor's Fellow** at *Quantum Software Lab (QSL), School of Informatics, University of Edinburgh*.

2022-2023 **Senior Researcher** at *The Laboratory for Foundations of Computer Science (LFCS), University of Edinburgh*.
I lead research on quantum hardware security, quantum pseudorandomness, quantum machine learning and distributed quantum computing.

2021-2022 **Research Associate** at *The Laboratory for Foundations of Computer Science (LFCS), University of Edinburgh*.
working on unclonability, cryptanalysis and quantum cryptography, quantum machine learning and quantum differential privacy.

2020-2021 **Research Intern** at *VeriQloud*, Mentor: Marc Kaplan
I worked as a research intern at VeriQloud, a quantum startup based in France, to conduct a feasibility study regarding the applications of quantum protocols and the quantum communication infrastructure in Europe.

2018-2020 **Quantum Protocol Zoo Contributor and Research Collaborator** *Quantum protocol zoo, is an open repository of protocols for quantum networks (https://wiki.veriqloud.fr)*. Within this project, I worked on the study, modularization and standardization of quantum protocols as part of the European Quantum Internet Alliance (QIA) project.

2014-2017 **Research Assistant**, Quantum Information and Computation Group, *Sharif University of Technology*,
I worked on various topics including quantum foundations, and no-go theorems and quantum resource theory.

Selected Awards and Honors

Jan 2022 **Hartree Fellowship**, *Awarded a highly competitive independent research fellowship at QUICS, Joint Center for Quantum Information and Computer Science, Maryland.*

Jan 2022 **Perimeter Institute Postdoctoral Fellowship**, *Awarded a highly competitive 3-year research fellowship at Perimeter Institute. (declined the offer)*

May 2020 **School winner of Three Minute Thesis**, *School of Informatics, University of Edinburgh.*

July 2019 **2nd place award in QuHackEd: The first Quantum Hackathon in Scotland**, *University of Edinburgh.*

Sep 2018 **Fully Funded PhD Scholarship**, *School of Informatics, University of Edinburgh.*

Selected Research Grant Contributions

QuantERA Grant: Hardware Security Module for secure delegated Quantum Cloud Computing (HSM-QCC), *CoI, Grant Amount: 1.2M EUR, UoE: 261K GBP*

Practical Quantum Cryptography from Hardware Assumptions - Cisco, *CoI, Grant Amount: 100K USD.*

AirQKD, *Contributor, project: "PUF-enhanced QKD authentication", Total Grant Amount: 7.5M GBP, UoE budget: 261K GBP.*

Quantum Computing Platform For NISQ Era Commercial Applications, *Contributor and sub-project leader, Grant Amount (UoE budget): 103K GBP.*

Quantum Internet Alliance, *Quantum protocol design work package contributor, student and intern supervisor, Total Grant Amount: 24M Euros.*

Selected Management Experience and Community Services

PC Member **PC member of** *Quantum Cryptography (QCrypt) conference 2024, 2-6 September 2024* - Vigo, Spain (Website link)

Organising committee **Local organising committee of QCTiP 2024** *Quantum Computing Theory in Practice, 16-18 April 2024* - University of Edinburgh (Website link)

Organising committee **Organiser of** *Quantum Hybrid and Hardware Security Workshop (22-23 November 2023)* - University of Edinburgh

Organising committee **Chair and organiser of** *International Workshop on Quantum t-designs and Applications in Quantum Computing, 23-25 March 2022* - University of Edinburgh (Website link)

Organising committee **co-organiser of** *Quantum Software Lab Workshop 13-14 December 2022* - University of Edinburgh (Website link)

Organising committee **Local organiser of** *4th National Conference of Superconductivity - 2014*, Sharif University of Technology

Reviewer Conferences: QCrypt, QIP, TQC, QCTiP
Journals: Nature Physics, npj Quantum Information, Advances in Mathematics of Communications, Quantum journal, ACM ToCL, PRA

Supervision

Current PhD students Chirag Wadhwa (started Sep 2023), Mario Herrero Gonzalez (will start Sep 2024), Tommy Williams (will start Sep 2024)

Current PhD students **(secondary-advisor)** Abbas Poshtvan, Stuart Fergusen

Current Interns Ben Priestley (Summer LFCS intern 2024)

Past Interns & Undergrad students Chirag Wadhwa, Natansh Mathur, Sara Sarfaraz, Magnus Kleinau

Selected Teaching Experience

Jan 2024 **Lecturer** *Quantum Cyber Security (QCS) SEM2 2024, University of Edinburgh, co-lectured with Petros Wallden*

Apr 2022 **Guest lecture** on "Quantum coin-flipping", *for the course "Quantum Cyber Security", Lecturer: Petros Wallden, University of Edinburgh.*

2019-2022 Teaching Assistant, **Quantum Mechanics**, *School of Physics and Astronomy, University of Edinburgh.*

2020-2021 Teaching Assistant, **Introduction to Modern Cryptography**, *School of Informatics, University of Edinburgh.*

2019-2021 Teaching Assistant, **Introduction to Quantum Computation**, *School of Informatics, University of Edinburgh.*

2019-2021 Teaching Assistant, **Dynamics and Vector Calculus**, *School of Physics and Astronomy, University of Edinburgh.*

2015-2016 Teaching Assistant, **Modern Physics**, *Department of Physics, Sharif University of Technology.*

Publications (Sorted by the most recent)

[1] Wadhwa, C., Doosti, M. (2024). Noise-tolerant learnability of shallow quantum circuits from statistics and the cost of quantum pseudorandomness. arXiv preprint arXiv:2405.12085.

[2] Singh, S., Doosti, M., Mathur, N., Delavar, M., Mantri, A., Ollivier, H. and Kashefi, E., 2023. Towards a unified quantum protocol framework: Classification, implementation, and use case. arXiv preprint arXiv:2310.12780

[3] Wadhwa, C. and Doosti, M. 2023 Learning quantum processes with quantum statistical queries. arXiv preprint arXiv:2310.02075

[4] Angrisani, A., Doosti, M. and Kashefi, E., 2023. A unifying framework for differentially private quantum algorithms. arXiv preprint arXiv:2307.04733.

[5] Doosti, M., Hanouz, L., Marin, A., Kashefi, E. and Kaplan, M., 2023. Establishing shared secret keys on quantum line networks: protocol and security. arXiv preprint arXiv:2304.01881.

[6] Doosti, M., Kumar, N., Kashefi, E., and Chakraborty K., 2022 On the connection between quantum pseudorandomness and quantum hardware assumptions. Quantum Science and Technology, 7(3):035004.

[7] Angrisani, A., Doosti, M., and Kashefi, E., 2022. Differential privacy amplification in quantum and quantum-inspired algorithms. arXiv preprint arXiv:2203.03604, 2022. **Accepted for oral presentation at ICLR 2022**

[8] Chakraborty, K., Doosti, M., Ma, Y., Wadhwa, C., Arapinis, M., and Kashefi, E., 2021-2. Quantum lock: A provable quantum communication advantage. arXiv preprint arXiv:2110.09469, 2021. **Accepted for publication at Quantum Journal, and for oral presentation at QCrypt 2022**

[9] Coyle, B., Doosti, M., Kashefi, E. and Kumar, N., 2022. Progress toward practical quantum cryptanalysis by variational quantum cloning. Phys. Rev. A, 105:042604, Apr 2022. **Accepted for oral presentation at YQIS 2021**

[10] Doosti, M., Delavar, M., Kashefi, E., and Arapinis, M., 2021. A Unified Framework For Quantum Unforgeability. arXiv preprint arXiv:2103.13994.

[11] Doosti, M., Kumar, N., Delavar, M. and Kashefi, E., 2021. Client-server identification protocols with quantum PUF. ACM Transactions on Quantum Computing, 2(3), pp.1-40.

[12] Arapinis, M., Delavar, M., Doosti, M., and Kashefi, E., 2021. Quantum physical unclonable functions: Possibilities and impossibilities. Quantum, 5, 475. **Accepted for oral presentation at QCrypt 2019**

[13] Doosti, M., Kianvash, F., and Karimipour, V. (2017). Universal superposition of orthogonal states. Physical Review A, 96(5), 052318.

Selected Talks

April 2024 "Unclonability and How it links quantum foundations to quantum applications", *Invited talk at Foundations of Quantum Computational Advantage (FoQaCiA) conference 2024, Perimeter Institute, Waterloo, Canada (online talk)*

March 2024 "From unclonability to learnability and quantum cryptography", *Invited seminar talk for Quantum Information Group at University of Tokyo, Japan (online talk)*

Jan 2024 "Quantum and Classical Cryptography meet New Resources", *Invited talk at Quantum Meets Classical Cryptography Paris, January 2024, France*

November 2023 "The Power of Unknown Unitaries", *Talk at Phoqusing workshop, Sorbonne University, LIP6, Paris, France*

September 2023 "New Resources for Quantum Communication: Exploring Quantum Hardware Security", *Invited talk at International Hub workshop on advances in quantum networking (QNetworks 2023), Glasgow, UK*

June 2023 "New quantum resources for quantum communication, from quantum hardware security", *Invited talk at Workshop on Entanglement Assisted Communication Networks, Taipei/Taiwan.*

April 2023 "Quantum cybersecurity and privacy", *Talk at the Quantum Software Lab launch event.*

March 2023 "New quantum resources from quantum hardware security for the NISQ era", *Invited talk Near-term Quantum Computing Conference 2023, Warsaw, Poland.*

March 2023 "Unclonability, learnability, and quantum pseudorandomness", *Invited talk at Royal Halloway University of London.*

Dec 2022 "Quantum Unclonability beyond no-cloning", *Quantum Software Lab workshop, University of Edinburgh.*

Jul 2022 "Security and Privacy in the quantum era", *Invited talk for Security and Privacy group at the School of Informatics, University of Edinburgh.*

Nov 2021 "Quantum Physical Unclonable Functions and Their Comprehensive Cryptanalysis", *IQC-QuICS Math-CS Seminar, Joint Center for Quantum Information and Computer Science*

Oct 2021 "From Quantum Computing to Quantum Mechanics: A journey backwards in time", *Invited public talk for Design Informatics, University of Edinburgh.*

Mar 2021 "Client-Server Identification Protocols with Quantum PUF", *Invited talk for Qtech QUISCO (Quantum Information Scotland Network) Seminar.*

Dec 2020 "Quantum Hardware Security, open questions and challenges", *Talk at Quantum Edi-Par workshop 2020 (Joint online workshop between University of Edinburgh quantum group and LIP6, Sorbonne University).*

Nov 2020 "Quantum Physical Unclonable Functions: Possibilities and Impossibilities", *Invited talk at University of Twente.*

Nov 2020 "Quantum Physical Unclonable Functions: Possibilities and Impossibilities", *Contributed talk at Quantum Technology International Conference 2020.*

Nov 2020 "Quantum Protocol Zoo", *Contributed talk at Quantum Technology International Conference 2020.*

Jun 2020 "Client-Server Identification Protocols with Quantum PUF", *Invited talk at Quantum Internet Alliance (QIA) online consortium.*

Aug 2019 "Quantum Physical Unclonable Functions: Possibilities and Impossibilities", *Contributed talk at QCrypt 2019.*

Jul 2019 "Quantum Emulation for Cryptanalysis", *Talk at Quantum Edi-Par workshop 2019, University of Edinburgh.*

May 2019 "Quantum Physical Unclonable Functions", *Invited talk at LIP6 weekly Seminar, Sorbonne University, Paris.*

May 2019 "Quantum Protocol Zoo", *Workshop talk at Quantum Internet Alliance (QIA) consortium, Lisbon.*

Mar 2019 "A Quantum Protocol Zoo for Quantum Internet", *Talk at LFCS Security and Privacy Seminar, University of Edinburgh.*

Aug 2021 "A Unified Framework For Quantum Unforgeability", *Poster presentation at QCrypt 2021.*

Jul 2021 "Client-Server Identification Protocols with Quantum PUF", *Poster presentation at TQC 2021.*

Feb 2021 "Variational Quantum Cloning: Improving Practicality for Quantum Cryptanalysis", *Poster presentation at QIP (Conference on Quantum Information Processing) 2021.*

Sep 2018 "Universal Superposition of Unknown Quantum States", *Poster presentation at IICQI (International Iran Conference on Quantum Information) 2018. - won Best poster award*

Outreach and Engagement Activities

Podcast Guest in S2E11 of the insideQuantum podcast, (Link to the episode)

Public talk "From Quantum Computing to Quantum Mechanics: A journey backwards in time", *Public talk for Design Informatics, University of Edinburgh.* (Link to the talk)

Miscellaneous "Head manager and organiser of *Music Festival of Physics Department*, Sharif University of Technology" for two years; "Member of the central council: *Scientific Society of Physics Department*, Sharif University of Technology"; Editorial Board of "Takaneh: The Student Journal of Physics", *Sharif University of Technology (2011-2013).*

Languages

English	Fluent
French	Advanced
Farsi(Persian)	Native