Mina Doosti

Curriculum Vitae

Informatics Forum, 10 Crichton St, Edinburgh EH8 9AB, UK
(+44) 7808592057
mdoosti@ed.ac.uk,minadoosti@gmail.com

Overview

I am a senior research associate at the University of Edinburgh and a Hartree Fellow at QUICS. As a researcher in quantum information sciences and cryptography, my focus is on the intersection of quantum computing with cryptography and learning theory. With over seven years of experience in the field, 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

2022-now **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

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 and Leadership Experience

Research Leadership **Co-founder** of a new field of research namely, *quantum hardware security*. Also **founded the research subgroup** of quantum hardware security within the EdiPar quantum lab, leading the research around this topic, opening new research directions such as *quantum identification based on hardware assumptions* and, supervising students and interns.

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

Selected Supervision Experience

I supervised several undergraduate students and research interns during my PhD and afterwards, including the following projects and dissertations:

UoE **PhD student co-supervision: Abbas Poshtvan**, PhD Topic: Quantum hardware security and quantum pseudorandomness

UoE & IIT Roorkee **Research Intern: Chirag Wadhwa**, Project Title: Implementation of quantum algorithms for learning unknown unitaries and applications in quantum cryptanalysis.

UoE & IIT Roorkee **B.Sc. and Intern Chirag Wadhwa**, Project Title: Machine learning-based attacks and modelling of hybrid quantum-classical Physical Unclonable Functions.

UoE & Sorbonne **Research Interns: Shraddha Singh, Natansh Mathur**, Project Title: Quantum Protocol Zoo.

Sorbonne (LIP6) **Research Intern: Sara Sarfaraz**, Project Title: Review and security analysis of quantum E-voting protocols

UoE **B.Sc. Dissertation Supervision: Magnus Kleinau**, Dissertation Title: Simulation of Quantum Emulation algorithm.

Selected Teaching Experience

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] 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.

[2] 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.

[3] 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**

[4] 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**

[5] 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**

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

[7] 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.

[8] 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**

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

Selected Oral and Poster Presentations

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 Holloway 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, Service, and Engagement Activities

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)

Reviewer QCrypt conference, Quantum journal, QIP conference, ACM ToCL, PRA.

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).*

Selected Professional Skills

Quantum Platforms Rigetti PyQuil, IBM Qiskit

Programming C, C++, C#, Python, Object Oriented Programming, JAVA, Mathematica, Matlab

Languages

English Fluent

French Advanced

Farsi(Persian) Native

References

Elham Kashefi

Institution LFCS, School of Informatics, Unversity of Edinburgh

Position Personal Chair in Quantum Computing

Contact ekashefi@inf.ed.ac.uk

Myrto Arapinis

Institution LFCS, School of Informatics, Unversity of Edinburgh

Position Reader

Contact marapini@inf.ed.ac.uk

Anne Broadbent

Institution University of Ottawa

Position Associate Professor

Contact abroadbe@uottawa.ca

Marc Kaplan

Institution VeriQloud

Position CEO

Contact kaplan@veriqloud.com