Dr Aydin Abadi
Email: aydin.abadi@ncl.ac.uk
Website: http://www.aydinabadi.com
School of Computing, Newcastle University.

Research Interests

- Security, Privacy, and Cryptography.
- Privacy in Machine Learning.
- Security of Online Payment Systems.
- Secure Multi-party Computation and Private Set Intersection (PSI).
- Blockchain Technology and Smart Contracts.
- Verifiable Computation.

Prize

- **UK—US Privacy Enhancing Technologies (PETs) Challenge Prize (2023)**— Awarded Joint **First** Prize
  - Due to our achievement, our STARLIT solution, and consequently UCL, have received recognition from prominent authorities.
  - Notably, both THE WHITE HOUSE and UK Government websites have acknowledged our success—an unprecedented milestone in the history of UCL.
  - We were honored to receive a congratulatory email from the President of UCL, recognizing and celebrating our achievements.
- **Nominated for the "Staff Excellence Awards" (University of Gloucestershire, 2021)**.
- **Euan Minto Prize**, awarded to the author of the best paper authored by a research student in the Computer Science Department (University of Strathclyde, 2015).

Education

- PhD in Computer Science (Apr 2013—Feb 2017). University of Strathclyde, UK.
- M.Sc. in Computer Science (Sep 2009—Feb 2011). University of Leeds, UK.
- B.Sc. in Computer Science (2000—2004). University of Lahijan, Iran.
- Diploma in Mathematics and Physics (2000), Iran.

Professional History

- May 2024—present: Lecturer, Newcastle University (full-time, permanent position).
- 2022—May 2024: Senior Research Fellow at University College London, UK (full-time).
- 2021—2022: Research Fellow at University College London, UK (full-time).
- 2020—2021: Lecturer in Cyber Security at the University of Gloucestershire, UK (full-time, permanent position).
- 2017—2020: Research Associate, At Blockchain Technology Lab, University of Edinburgh, UK (full-time).
- 2005—2009: Software Engineer, Fardad Shomal Co., Iran (full-time, permanent position).

Selected Invited Talks and Interviews

- Title: "Delegated Time-Lock Puzzle", Nethermind (blockchain) Summit, Istanbul, 2023.
  - The recording is available through this link.
- Title: "Dealing with Online Banking and Cryptocurrency Fraud", UK--Kuwait Cybersecurity Education & Research Conference, Kuwait, 2023.
- Title: "Private Set Intersection with Reward Mechanisms", Royal Holloway University, 2023.
- Title: "Delegated Generic Multi-instance Time-lock Puzzle", University of Oxford, 2023.

- Title: “Recurring Contingent Service Payment”, interviewer: Faculti Media Limited, 2022.
- Title: “Polynomial representation is Tricky”, The UK Security and Privacy Seminar (UK-SPS), 2021.
    - The recording is available through this link.

Other Affiliations and Enterprise Engagement

- Associate member of Blockchain Technology Lab, University of Edinburgh, 2020—present.
- Technical consultant to Lyzis Labs (a start-up in the domain of Blockchain-based market), 2022—present.

Impact

- Lyzis Labs, a start-up, is currently developing the solutions that we introduced in our papers (accessible via, this, this, and this links).
    - The objective is to establish a secure, private, and transparent decentralized marketplace, minimizing dependence on a central authority. Essentially, the vision is to create a decentralized counterpart to platforms like eBay or Amazon.
    - The solutions are also designed to address the issue of counterfeit items, focusing on effective prevention and detection measures.

Selected Academic Service

- PC member of “the web conference” (a.k.a. www), 2022 and 2023.
- PC member of “InsCrypt” conference, 2023.
- PC member of “The Security Track” at the “ACM Symposium on Applied Computing” (SEC@SAC) 2024.
- Session chair at “ACM AsiaCCS” conference, 2023.
- Session chair at “Workshop on Timed-Release Encryption and its Applications”, University of Oxford, 2023.
- Reviewer journals and conferences such as: Journal of Mathematics’24, PKC’24, IEEE TDS’24, Transaction of Consumer Electronics (TCE) 2023, Symposium on Applied Computing (SAC) 2023, IEEE TDS’23, InsCrypt’23, PETs’22, IEEE TCC’22, AsiaCCS’22, ESORICS’22, IEEE TDSC’22, IEEE T-IFS’21, PETs’21, PKC’2020, CCS’19, EEE TDSC’18, TCC’18, FC’18, and Crypto’18.
- Member of “UCL Computer Science Ethics Committee”, 2022—present.
- Member of the “REPHRAIN College of Peer Reviewers”, 2022—present.
- Office space coordinator/champion, UCL, 2022—present.

Industry Partnership

- Privitar: Together with Privitar and a team from UCL, I led the development of a privacy-preserving Federated Learning-based solution, Starlit, documented in a published paper accessible via this link.

- Lyzis Labs: In partnership with Lyzis Labs, alongside teams from the University of Oxford and Pennsylvania State University, I contributed to the creation of a solution addressing counterfeit items. This collaborative effort resulted in several paper publications, and plans are underway to transform the solution into a market-ready product.
    - I have been presented with the opportunity to assume the role of Chief Technology Officer (CTO) at Lyzis Labs, a proposition that is presently under deliberation.

Public Engagement

- Financial Conduct Authority (FCA): Ensuring ongoing communication with FCA to apprise them of the outcomes and advancements stemming from our research on addressing online financial fraud.

- British Embassy in Kuwait: Sustaining regular communication with the British Embassy in Kuwait has been a priority. Noteworthy engagements include my invitation to a conference in Kuwait, attended by around 500 participants from the Kuwaiti government, academia, and industry. Additionally, I collaborated with Kuwait University to develop a research grant proposal, currently undergoing review.

Teaching

- Privacy-Enhancing Technologies (MSc), teaching assistant, UCL, 2021—present.
- Blockchain Technology and its Applications (MSc), **module leader**, University of Gloucestershire, 2020 & 2021.
- Introduction to Cryptography and Information Security (BSc & MSc), **module leader**, University of Gloucestershire, 2020 & 2021.
- Introduction to Programming Fundamentals (BSc), **module leader**, University of Gloucestershire, 2021.
- Project Management (BSc), **module leader**, University of Gloucestershire, 2021.
- Smart Contracts and Law (MSc), summer school, guest lecturer, University of Edinburgh, 2019.
- Blockchain Technology, Smart Contracts, and their Applications (MSc and PhD), teaching assistant, University of Edinburgh, 2018.

Selected Students Supervision

- Advising and collaborating with three PhD students; namely Lorenzo Martinico and Amirreza Sarencheh from the University of Edinburgh (2020—present) and Alireza Kavousi from UCL (2022—present).
- Supervised MSc projects, such as Afiq Samsudin and Eleni Sereli, 2022—2023.
- Supervised a BSc project supervision, University of Gloucestershire (2020).
- Hired and supervised two MSc students to build the decentralized ID management system, at the University of Edinburgh, (2019—2020).

Funding Received

- UK PETs Prize Challenge, the total budget £120k (2022—2023)—Co-I.

- REPHRAIN 3rd Strategic Funding Call, total budget £120k (2023)—Co-I.
  - Title: "Protecting (Young) Victims of Cryptocurrency Fraud": This project aims to develop a blockchain-based insurance mechanism that charges users a certain amount of premium and compensates them if they fall victim to cryptocurrency fraud.

- Led the following Research and Development (R&D) projects.
  - Project 1: Privacy-preserving Identity Management System (2019—2021).
    - Attracted internal funding: £70k.
    - End product: online blockchain-based platform, available via this link.
  - Project 2: A Blockchain-based Trading Platform to Encourage Student Engagement in Higher Education (2018—2020)
    - Attracted internal funding: £10k.
    - End product: online blockchain-based platform, available through this link.

Recent Funding Application Under Review

- Kuwait Foundation for the Advancement of Sciences (KFAS), 2023, the budget requested: £130k.

Involvement in Large-Scale Projects

- FENTEC (2019—2020), University of Edinburgh: I was a member of the research team in this project, funded by the European Union's Horizon 2020 Research and Innovation Programme (total allocated budget: €4,223,141). My role included conducting research and developing efficient (Functional and time-lock) encryption schemes.
- Oxchain (2017—2019), University of Edinburgh: I was a core member of the R&D team in the OxChain project, funded by EPSRC (total allocated budget: £992,269). My role included research in blockchain technology and developing decentralized applications and smart contracts.

Selected Open-Source Software

- **Privacy-preserving Identity Management System** (2019—2021). Developed and maintained an open-source Identity Management System with a focus on privacy preservation. This platform finds practical application in the banking sector, particularly in streamlining the "Know Your Customer" (KYC) process. Not only does it significantly reduce KYC verification costs, but it also carries the potential for substantial economic impact. The platform is accessible online via this link.
- **ValuED: A blockchain-based trading platform to encourage student engagement in higher education** (2019—2020). This innovative platform has been meticulously designed to stimulate and facilitate enhanced participation in academic pursuits, ultimately enhancing the overall student experience. To explore this platform further, it is accessible online via this link.
- **Multi-party Updatable Delegated Private Set Intersection** (2019—2022). The prototype has been created to enable parties to leverage the computational and storage capabilities of cloud computing while ensuring the confidentiality of their sensitive data. This specific variant of Private Set Intersection (PSI) empowers distinct parties to securely store their sensitive information in the cloud, delegating the computation of PSI without limitations. Notably, this software boasts scalability, efficiently managing thousands of clients, and holds promise for applications in Vertical Federated Learning due to its effectiveness and scalability. For those interested in exploring further, the source code can be accessed via this link.
- **For all software and libraries** that I have developed, see my GitHub repository via this link.

Other Profiles

- Google Scholar can be found via this link.
- GitHub profile can be found through this link.
- The personal website can be found via this link.
- DBLP profile can be accessed through this link.

Publications and 4 Selected Publications (marked by *)

- Journal Paper (refereed)
  - * "**Efficient delegated private set intersection on outsourced private datasets**"
    - Aydin Abadi (first author), Sotirios Terzis, Roberto Metere, Changyu Dong
    - In IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, Volume 16, Issue 4. Impact Factor: 7.3.
    - Access the paper via this link.

- Conference Papers (refereed)
  - "**Recurring Contingent Service Payment**"
    - Aydin Abadi (first author), Steven J. Murdoch, Thomas Zacharias.
    - In IEEE European Symposium on Security and Privacy (Euro S&P), 2023, the Acceptance Rate: 22%.
    - Access the paper via this link.

  - * "**Payment with Dispute Resolution: A Protocol For Reimbursing Frauds Victims**"
    - Aydin Abadi (first author), Steven J. Murdoch
    - In ACM ASIA Conference on Computer and Communications Security (AsiaCCS) 2023, the Acceptance Rate: 18%.
    - Access the paper via this link.

  - "**An Efficient and Decentralized Blockchain-based Commercial Alternative**"
    - Marwan Zeggari, Renaud Lambiotte, Aydin Abadi
    - In IEEE 20th International Conference on Software Architecture Companion (ICSA-C), 2023.
    - Access the paper via this link.

- * "**Multi-party Updatable Delegated Private Set Intersection**"
  - Aydin Abadi (first author), Changyu Dong, Steven J. Murdoch, Sotirios Terzis
- In Financial Cryptography and Data Security (FC), 2022, the Acceptance Rate: 21.3%.
  - Access the paper via this link.

- * "**Multi-instance Publicly Verifiable Time-lock Puzzle and its Applications**"
  - Aydin Abadi (first author), Aggelos Kiayias
- In Financial Cryptography and Data Security (FC), 2021, the Acceptance Rate: 24.2%.
  - Access the paper via this link.

- "**Polynomial Representation Is Tricky: Maliciously Secure Private Set Intersection Revisited**"
  - Aydin Abadi (first author), Steven J. Murdoch, Thomas Zacharias
  - In European Symposium on Research in Computer Security (ESORICS), 2021, the Acceptance Rate: 20.2%.
  - Access the paper via this link.

- "**Timed Signatures and Zero-Knowledge Proofs—Timestamping in the Blockchain Era**"
  - Aydin Abadi, Michele Ciampi, Aggelos Kiayias, Vassilis Zikas
  - In Applied Cryptography and Network Security (ACNS), 2021, the Acceptance Rate: 21.5%.
- Access the paper via this link.

- "**Smart Donations: Event-Driven Conditional Donations Using Smart Contracts On The Blockchain**"
  - Ludwig Trotter, Mike Harding, Peter Shaw, Nigel Davies, Chris Elsden, Chris Speed, John Vines, Aydin Abadi, Josh Hallwright
  - In Australian Conference on Human-Computer Interaction (OZCHI), 2020, the Acceptance Rate: 45%.
  - Access the paper via this link.

- "**VD-PSI: verifiable delegated private set intersection on outsourced private datasets**"
  - Aydin Abadi (first author), Sotirios Terzis, Changyu Dong
  - In Financial Cryptography and Data Security (FC), 2016, the Acceptance Rate: 26.2%.
  - Access the paper via this link.

- "**O-PSI: delegated private set intersection on outsourced datasets**" **—Won the prize for the best paper authored by a student, i.e., Euan Minto Prize.**
  - Aydin Abadi (first author), Sotirios Terzis, Changyu Dong
  - In IFIP International Information Security and Privacy Conference (SEC), 2015, the Acceptance Rate: 19.8%.
  - Access the paper via this link.

- Book Chapter (refereed)

  - "**Smarter Data Availability Checks in the Cloud: Proof of Storage via Blockchain**"
    - Aydin Abadi
  - In Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies, 2022, IGI Global.
  - Access the chapter via this link.

- Preprints
  - **“Starlit: A Privacy-Preserving Vertical Federated Learning to Enhance Financial Fraud Detection”—Won UK-US PETS Prize**
    - Aydin Abadi, Bradley Doyle, Francesco Gini, Kieron Guinamard, Sasi Kumar Murakonda, JackLiddell, Paul Mellor, Steven J. Murdoch, Mohammad Naseri, Hector Page, George Theodorakopoulos, Suzanne Weller Theodorakopoulos, Suzanne Weller
    - In Cryptology ePrint Archive, 2024
    - Access the paper via this link.

  - “**Delegated-Query Oblivious Transfer and its Applications**”
    - Aydin Abadi (first author), Yvo Desmedt
    - In GitHub Archive, 2024 (under review by TDSC’24)
    - Access the paper via this link.

  - “**Earn While You Reveal: Private Set Intersection that Rewards Participants**”
    - Aydin Abadi
    - In Cryptology ePrint Archive, 2023
    - Access the paper via this link.

  - “**Decentralised Repeated Modular Squaring Service Revisited: Attack and Mitigation**”
    - Aydin Abadi
    - In Cryptology ePrint Archive, 2023
    - Access the paper via this link.

  - **“Delegated Time-Lock Puzzle”**
    - Aydin Abadi (first author), Dan Ristea, Steven J. Murdoch
    - In Cryptology ePrint Archive, 2023
    - Access the paper via this link.

  - “**A Forward-secure Efficient Two-factor Authentication Protocol**”
    - Steven J. Murdoch, Aydin Abadi
    - In Cryptology ePrint Archive, 2022.

- Access the paper via this link.

  - “**Timed Secret Sharing**”
    - Alireza Kavousi, Aydin Abadi, Philipp Jovanovic
    - In Cryptology ePrint Archive, 2023
    - Access the paper via this link.

  - **“REPHRAIN White Paper: the Metaverse and Web 3.0”**
    - Aydin Abadi, Madeline Carr, Ignacio Castro, Alicia Cork, Andrés Domínguez, Cristina Fiani, Mohamed Khamis, Mark McGill, Steven J Murdoch, Awais Rashid, Pejman Saeghe, Gareth Tyson
    - Access the paper via this link.

  - **“Safeguarding Physical Sneaker Sale Through a Decentralized Medium”**
    - Marwan Zeggari, Aydin Abadi, Renaud Lambiotte, Mohamad Kassab
    - In Computing Research Repository (CORR), 2023
    - Access the paper via this link.

  - “**Glass-Vault: A Generic Transparent Privacy-preserving Exposure Notification Analytics Platform**”

- Lorenzo Martinico, Aydin Abadi, Thomas Zacharias, Thomas Win.
- In Computing Research Repository (CORR), 2022 (under review by AsiaCCS'24)
- Access the paper via this link.

- "**Recurring Contingent Payment for Proofs of Retrievability**"
  - Aydin Abadi (first author), Steven J. Murdoch, Thomas Zacharias
  - In Cryptology ePrint Archive, 2021.
  - Access the paper via this link.

- "**ValuED: A Blockchain-based Trading Platform to Encourage Student Engagement in Higher Education**"
  - Aydin Abadi (first author), Jin Xiao, Roberto Metere, Richard Shillcock.
  - PsyArXiv, 2021.
  - Access the paper via this link.

Referees

- Prof. Steven Murdoch (current line manager)
  - Royal Society University Research Fellow and Head of the Information Security Research Group at UCL. He is also a bye-fellow of Christ's College and a Fellow of the IET and BCS.
  - Email: s.murdoch@ucl.ac.uk
- Prof. Yvo Desmedt (academic partner)
  - Jonsson Distinguished Professor at the University of Texas at Dallas.
  - Email: y.desmedt@cs.ucl.ac.uk
- Prof. Aggelos Kiayias (previous line manager)
  - Fellow of the Royal Society of Edinburgh (FRSE), Chair in Cyber Security and Privacy, and Director of the Blockchain Technology Laboratory at the University of Edinburgh. He is also the Chief Scientist at a blockchain technology company, called IOHK.
  - Email: aggelos.kiayias@ed.ac.uk
- Prof. Madeline Carr (academic colleague)
  - Director of the Research Institute in Sociotechnical Cyber Security (RISCS), and Director of the Digital Technologies Policy Lab.
  - Email: m.carr@ucl.ac.uk
- Prof. Awais Rashid (academic partner)
  - Head of Bristol Cyber Security Group and Director of National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN).
  - Email: awais.rashid@bristol.ac.uk
- Prof. Changyu Dong (previous PhD supervisor)
  - Director of Research Institute of AI and Blockchain, Guangzhou University.
  - Email: changyu.dong@gmail.com