Dr Aydin Abadi
Email: aydin.abadi@ucl.ac.uk
Department of Computer Science, UCL.
http://www.aydinabadi.com

Research Interests.

- Security, Privacy, and Cryptography.
- Security of Online Banking.
- Blockchain Technology.
- Private Set Intersection (PSI).
- Verifiable Computation.

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.

Prize.

- **UK Privacy Enhancing Technologies (PETs) Challenge Prize (2022)**.
- **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).

Professional History.

- Senior Research Fellow, UCL, May 2021--present.
- Lecturer in Cybersecurity, University of Gloucestershire, Oct 2020--May 2021.
- Research Associate, Blockchain lab, University of Edinburgh, Jun 2017--Sep 2020.
- IT Manager, Komite Emdad, Iran, 2007--2009.
- Hardware Engineer, Fardad Shomal Co., Iran, 2005--2007.

Other Affiliations.

- Associate member of Blockchain Technology Lab, University of Edinburgh, 2020--present.
- Member of REPHRAIN.

Key Open-source Software.

- **Privacy-preserving Identity Management System** (2019--2021). A concrete application of this platform is in banking where the process of "Know Your Customer" (KYC) plays a crucial role. This platform reduces KYC verification costs and has a potential economic impact. The platform is available online in [1].
- **ValuED: A blockchain-based trading platform to encourage student engagement in higher education** (2019--2020). It has been designed to provoke and facilitate students' engagement in higher education. It has the potential to improve students' experience. The platform is available online [2].

Enterprise\External Engagement.

- I am a technical advisor to Lyzis Labs (a start-up in the domain of Blockchain-based market), 2022--present.
- I am a technical advisor to Privitar on "STARLIT" project, 2022--present.

Funding Received.

- UK PETs Prize Challenge, the total budget that our team received was £60k (2022).

Recent Funding Sought.

- Royal Society University Research Fellowship, 2022, the budget requested: £1.2m.

- EPSRC Open Fellowship, 2022, the budget requested: £1.3m, under review.
- REPHRAIN 3rd Strategic Funding Call, 2022, the budget requested: £120k, under review.

Key Publications. In the publications listed below, the lead author is listed first.

- Journal paper (refereed)
  - "**Efficient delegated private set intersection on outsourced private datasets**"
    Aydin Abadi, Sotirios Terzis, Roberto Metere, Changyu Dong
    In IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, Volume 16, Issue 4.
- Contributions to symposia and compiled volumes (refereed)
  - "**An Efficient and Decentralized Blockchain-based Commercial Alternative**"
    Marwan Zeggari, Renaud Lambiotte, Aydin Abadi
    In Blockchain Architecture (BlockArch) workshop, 2023.
  - "**Multi-party Updatable Delegated Private Set Intersection**"
    Aydin Abadi, Changyu Dong, Steven J. Murdoch, Sotirios Terzis
    In Financial Cryptography and Data Security (FC), 2022, Acceptance rate: 21.3%.
  - "**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.
  - "**Multi-instance Publicly Verifiable Time-lock Puzzle and its Applications**"
    Aydin Abadi, Aggelos Kiayias
    In Financial Cryptography and Data Security (FC), 2021, Acceptance rate: 24.2%.
  - "**Polynomial Representation Is Tricky: Maliciously Secure Private Set Intersection Revisited**"
    Aydin Abadi, Steven J. Murdoch, Thomas Zacharias
    In European Symposium on Research in Computer Security (ESORICS), 2021, Acceptance rate: 20.2%.
  - "**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, Acceptance rate: 21.5%.
  - "**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, Acceptance rate: 45%.
  - "**VD-PSI: verifiable delegated private set intersection on outsourced private datasets**"
    Aydin Abadi, Sotirios Terzis, Changyu Dong
    In Financial Cryptography and Data Security (FC), 2016, Acceptance rate: 26.2%.
  - "**O-PSI: delegated private set intersection on outsourced datasets**"
    Aydin Abadi, Sotirios Terzis, Changyu Dong
    In IFIP International Information Security and Privacy Conference (SEC), 2015, Acceptance rate: 19.8%.