Personal information

Name / Surname	**PASSERAT-PALMBACH Jonathan**
Personal Email	j.passerat-palmbach@imperial.ac.uk
Last Update	14-feb-2024
Web page	https://jopasser.at

Current Position

Since 2022	**Senior Research Scientist at Flashbots, London, United Kingdom** *Exploring the application of Privacy Enhancing Technologies to address the centralisation effects of Maximum Extractable Value (MEV) in blockchains*
Research Topics	Secure Computing (Intel SGX, Homomorphic Encryption) Verifiable Computing (Trusted Execution Environments, Zero-Knowledge Proofs) Crypto x AI

Other affiliations

Since 2014	**Research Fellow at Imperial College, London, United Kingdom**
Research Topics	Federated Learning Privacy-Preserving Machine Learning
Since 2022	**Honorary Research Fellow at City University, London, United Kingdom** Actively engaged in the co-supervision of a PhD student in **Federated Learning**, offering both guidance and collaboration on various publications.

Education

2010-2013	**PhD in Computer Science**
Title	*Contributions to Parallel Stochastic Simulation: Application of Good Software Engineering Practices to the Distribution of Pseudorandom Streams in Hybrid Monte-Carlo Simulations* Defended on October, 11th 2013
College	Engineering Doctoral School, Blaise Pascal University, Clermont-Ferrand, France
Research laboratory	CNRS - UMR 6158 LIMOS
Advisors	Prof. David R.C. Hill, Dr. Claude Mazel, Dr. Bruno Bachelet

Awards

Foresight Fellowship	**Private and Verifiable Machine Learning**
Best Paper Award	European Simulation and Modeling (ESM) Conference, Guimares, Portugal
Best Scientific Contribution	Yearly Seminar of the Engineering Doctoral School, Blaise Pascal University, Clermont-Ferrand, France

Grants

iEx.ec DApp challenge	Received $20,000 to support the integration of the **iEx.ec computing resources market place** in the OpenMOLE scientific platform
AWS Research grants	Support the distribution of large scale connectomics experiments using the Human Connectome Project dataset
NSF SBIR	Pitch accepted, proposal under development

Community Service

Conference organisation

2021	Secure and **Privacy-Preserving Machine Learning for Medical Imaging**: MICCAI 2021 Workshop and Tutorial
2020	**IEEE AIChain**: International Workshop on Advances in Artificial Intelligence for Blockchain
2016-	**BACON**: Workshop on Brain Analysis using COnnectivity Networks, satellite event of **MICCAI**
2016	Big Data in Medical Imaging, special session of **ISBI**

2015	Symposium on Big Data Initiatives for Connectomics Research, satellite event of the International conference on **Brain Informatics and Health**

Reviewer

Nature Computational Intelligence, Nature Scientific Communications
Patterns (Cell Press)
Journal of Machine Learning Research (JMLR)
IEEE Transactions on Medical Imaging (TMI)
Privacy Preserving Machine Learning in Practice @CCS 2020
NeurIPS Privacy and Fairness workshops 2022-
IEEE ISBI 2024
IEEE AIChain
IEEE ZKDapps
AAAI PPAI workshop

Editorial roles

Associate editor Blockchain for Science - Frontiers in Blockchain
Research Topic editor Blockchain for Health Data Sharing Systems to Accelerate Precision Medicine and Therapeutic Development - Frontiers in Blockchain

Teaching and Scientific Seminars

Teaching

2022	**Zero-Knowledge Proofs for Machine Learning**
10h	Pre-requisite to ZKML student projects
2016	**Functional programming in Haskell**
10h	1st year computing undergraduate, Imperial College London
2016	**Introduction to Java**
10h	1st year computing undergraduate, Imperial College London
2010-2013	**EGI Computing Grid labs**
10h	3rd year ISIMA (Computer Science Engineering School)
2010-2013	**High Performance Computing course**
4h	MRes in Computer Science, Blaise Pascal University
2012-2013	**GPU Computing course**
16h	3rd year ISIMA (Computer Science Engineering School)
2010-2013	**C++ labs**
16h + 16h	2rd & 3rd year ISIMA (Computer Science Engineering School)
2010-2011	**Java course**
22h	2nd year ISIMA (Computer Science Engineering School)
2010-2011	**Software Engineering**
16h	1st year BSc in Computer Science, Blaise Pascal University
2010-13	**UML tutorials**
8h	2nd year ISIMA (Computer Science Engineering School)

Recent Supervision

2023	**Verifiable Inference with Zero-Knowledge Proofs (ZKML)**, Bianca Ganescu (MEng student in Computer Science, Imperial College London, UK)
2022-	**Federated Learning for Medical Imaging**, Vasilis Siomos (PhD Computer Science, City University, London, UK)
2020-	**Adversarial Machine Learning**, Dmitrii Usynin (PhD Computer Science, Imperial College London, UK)
2019	**AutoML - Hyperparameter tuning and Neural Architecture Search**, Cristian Matache and Maurizio Zen (MEng Computer Science, Imperial College London, UK)
2018	**Federated machine learning on medical data using blockchain technology**, Théo Ryffel (MSc student in Computer Science, Imperial College London, UK / École Polytechnique, France)

Invited Talks

2023	**0xAI: The Odd Couple: How Can Blockchain Help AI**, panel at Chainlink's SmartCon, Barcelona, Spain
2023	**Privacy x MEV: mitigating, empowering, distributing**, RedChain Labs Workshop, Lyon, France
2023	**Joys and Challenges of Adopting PETs**, Flashbots Privacy Roast, online
2021	**Where is Trust in the age of no Trust? - Hardware vs. Software-Based Trusted Compute Approaches**, EEA Trusted Compute WG Monthly Webinar, *joint-talk with Andreas Freund*, online
2021	**No Country for Old Data - Data Valuation Considerations for AI/ML**, IEEE Healthcare: Blockchain & AI Virtual Series presents Healthcare Data Valuation, online
2021	**Privacy Preserving Machine Learning & Decentralisation**, FCA's AI Talks – Academic Series, online
2020	**Secure Computing solutions for Healthcare**, CitAI seminar series, City University London, UK
2019	**Convergence of Blockchain and Secure Computing for Healthcare solutions**, EU Blockchain forum, Frankfurt, Germany

Skills

Languages	English (fluent), French (mother tongue)
Computer Science	
Programming Languages	C, C++, Java, CUDA, Scala, Bash, **Python**, Solidity, **Rust**
Software Engineering Tools	Git, CMake, Maven, Valgrind, GDB, Puppet, Salt, SBT
Operating System	GNU Linux (Debian/Ubuntu)
Job Schedulers	EMI, PBS/Torque, Slurm
Distributed Filesystems	Ceph, GlusterFS
Web3	**Ethereum**, MEV, IPFS
Cryptography	**Intel SGX**, ZK Proofs, Multi-Party Computation, **Homomorphic Encryption**
Sport	
Karate	Distinguished athlete (national and international medallist) Member of the England National A Squad Black Belt (4^{th} dan) Professional instructor degree

Selected Publications

Complete list available at https://orcid.org/0000-0003-3178-9502

[1] Bianca-Mihaela Ganescu and **Jonathan Passerat-Palmbach**.
Trust the process: Zero-knowledge machine learning to enhance trust in generative ai interactions, 2024.
AAAI 2024- Privacy-Preserving AI Workshop.

[2] V Siomos, S Naval-Marimont, **Jonathan Passerat-Palmbach**, and G Tarroni.
Aria: On the interaction between architectures, aggregation methods and initializations in federated visual classification, Nov 2023.
21st IEEE International Symposium on Biomedical Imaging.

[3] X Sun, D Crapis, M Stephenson, B Monnot, T Thiery, and **Jonathan Passerat-Palmbach**.
Cooperative ai via decentralized commitment devices, Nov 2023.
NeurIPS 2023- Multi-Agent Security Workshop.

[4] G-L Pereteanu, A Alansary, and **Jonathan Passerat-Palmbach**.
Split he: Fast secure inference combining split learning and homomorphic encryption, Feb 2022.

[5] Dmitrii Usynin, Georgios Kaissis, and **Jonathan Passerat-Palmbach**.
Zen and the art of model adaptation: Low-utility-cost attack mitigations in collaborative machine learning.
Proceedings on Privacy Enhancing Technologies, 2022.

[6] V Siomos and **Jonathan Passerat-Palmbach**.
Contribution evaluation in federated learning: Examining current approaches, December 2021.
Published at New Frontiers in Federated Learning: Privacy, Fairness, Robustness, Personalization and Data Ownership workshop @NeurIPS 2021.

[7] Georgios Kaissis, Alexander Ziller, **Jonathan Passerat-Palmbach**, Théo Ryffel, Dmitrii Usynin, Andrew Trask, Ionésio Lima, Jason Mancuso, Friederike Jungmann, Marc-Matthias Steinborn, et al.
End-to-end privacy preserving deep learning on multi-institutional medical imaging.
Nature Machine Intelligence, 3(6):473–484, 2021.

[8] Ashly Lau and **Jonathan Passerat-Palmbach**.
Statistical privacy guarantees of machine learning preprocessing techniques.
2021 Workshop on Theory and Practice of Differential Privacy, 2021.

[9] Dmitrii Usynin, Alexander Ziller, Marcus Makowski, Rickmer Braren, Daniel Rueckert, Ben Glocker, Georgios Kaissis, and **Jonathan Passerat-Palmbach**.
Adversarial interference and its mitigations in privacy-preserving collaborative machine learning.
Nature Machine Intelligence, 2021.

[10] Veneta Haralampieva, Daniel Rueckert, and **Jonathan Passerat-Palmbach**.
A systematic comparison of encrypted machine learning solutions for image classification.
Proceedings of the 2020 Workshop on Privacy-Preserving Machine Learning in Practice, Nov 2020.

[11] Harry Cai, Daniel Rueckert, and **Jonathan Passerat-Palmbach**.
2cp: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments.
IEEE 2nd International Workshop on Advances in Artificial Intelligence for Blockchain, 2020.

[12] Theo Ryffel, Andrew Trask, Morten Dahl, Bobby Wagner, Jason Mancuso, Daniel Rueckert, and **Jonathan Passerat-Palmbach**.
A generic framework for privacy preserving deep learning.
CoRR, abs/1811.04017, 2018.