Sinem Sav
Bilkent University, EA 523
Ankara 06800, Turkey
+90 (554) 2338120, sinem.sav@cs.bilkent.edu.tr

CURRENT POSITION

Bilkent University, Ankara, Turkey — 2023 - ongoing
Assistant Professor, Computer Engineering Department

EDUCATION

École Polytechnique Fédérale de Lausanne (EPFL), Switzerland — 2018 - 2023
PhD, in School of Computer and Communication Sciences
Advisor: Prof. Jean-Pierre Hubaux, Prof. Carmela Troncoso

Bilkent University, Ankara, Turkey — 2016 - 2018
Master of Science, in Computer Engineering
Advisor: Prof. Erman Ayday
CGPA 3.91

Bilkent University, Ankara, Turkey — 2012 - 2016
Bachelor of Science, in Computer Engineering
CGPA 3.66

RESEARCH INTEREST

Privacy enhancing technologies, applied cryptography, big data privacy, privacy-preserving machine learning, federated learning, multiparty homomorphic encryption, biomedical/genomic data privacy.

WORK EXPERIENCE

HAVELSAN Inc., Ankara, Turkey — September 2016 - March 2018
Industry Project
Privacy-Preserving Medical Databases, application of Paillier cryptosystem and homomorphic operations to health informations.

HAVELSAN Inc., Ankara, Turkey — April 2016 - July 2016
Software Engineer (Candidate) Command Control and Combat Systems

Simon Fraser University, BC, Canada — June 2015 - September 2015
Undergraduate Research Assistant, on RNA-Design problem with simulated-annealing
Advisor: Prof. Herbert H. Tsang

TAI, Turkish Aerospace Industry Inc., Ankara, Turkey — June 2014 - July 2014
Intern, IT department.

TEACHING EXPERIENCE

Teaching Assistant — Fall 2014 - Present
Bilkent University, Computer Science Department, Ankara, Turkey

- Algorithms and Programming I-Java (CS-101).
- Introduction to Programming for Engineers - Java (CS-114).
- Software Architecture Design (CS-411).
- Object Oriented Programming (CS-319).

EPFL, School of Computer and Communication Sciences

- Information Security and Privacy (COM-402).
- Mobile Networks (COM-405).
- Advanced Topics on Privacy Enhancing Technologies (CS-523)

JOURNAL PUBLICATIONS

- Sinem Sav, Abdulrahman Diaa, Apostolos Pyrgelis,, Jean-Philippe Bossuat, and Jean-Pierre Hubaux
  Privacy-Preserving Federated Recurrent Neural Networks.
  Proceedings on Privacy Enhancing Technologies (PoPETs), 2023(4).
- Sinem Sav, Jean-Philippe Bossuat, Juan R. Troncoso-Pastoriza, Manfred Claassen, and Jean-Pierre Hubaux
  Privacy-Preserving Federated Neural Network Learning for Disease-Associated Cell Classification.
  Patterns, 3(5), 2022.
- David Froelicher, Juan R. Troncoso-Pastoriza, Apostolos Pyrgelis, Sinem Sav, Joao Sa Sousa, Jean-Philippe Bossuat, and Jean-Pierre Hubaux
  Scalable Privacy-Preserving Distributed Learning. *Proceedings on Privacy Enhancing Technologies (PoPETs), 2021(2).*

CONFERENCE PUBLICATIONS

- Sinem Sav, Apostolos Pyrgelis, Juan R. Troncoso-Pastoriza, David Froelicher, Jean-Philippe Bossuat, Joao Sa Sousa, and Jean-Pierre Hubaux
  POSEIDON: Privacy-Preserving Federated Neural Network Learning.
  Network and Distributed Systems Security (NDSS) Symposium, 2021.
  Selected as the best paper in CSAW'21 Applied Research Competition in Europe.
  Selected talk for PPML NeurIPS, 2020.
- Sinem Sav, David Hampson, and Herbert H. Tsang,
  SIMARD: A Simulated Annealing Based RNA Design Algorithm with Quality Pre-Selection Strategies. *IEEE Symposium Series on Computational Intelligence (SSCI), 2016.*
- Halid Emre Erhan, Sinem Sav, Stas Kalashnikov, and Herbert H. Tsang,
  Examining the Annealing Schedules for RNA Design Algorithm. *IEEE Congress on Evolutionary Computation, July 24-29, 2016.*
- David Hampson, Sinem Sav, and Herbert H. Tsang,
  Investigation of Multi-Objective Optimization Criteria for RNA Design.
  IEEE Symposium Series on Computational Intelligence (SSCI), 2016.

WORKSHOP PUBLICATIONS

- Francesco Intoci*, Sinem Sav*, Apostolos Pyrgelis, Jean-Philippe Bossuat, Juan R. Troncoso-Pastoriza, and Jean-Pierre Hubaux
  SlytHErin: An Agile Framework for Encrypted Deep Neural Network Inference
  Accepted at 5th Workshop on Cloud Security and Privacy (Cloud S&P 2023) co-located with ACNS.

PATENTS

- David Froelicher, Juan Ramón Troncoso-Pastoriza, Apostolos Pyrgelis, Sinem Sav, Joao André Gomes de Sá e Sousa, Jean-Pierre Hubaux, Jean-Philippe Bossuat
  System and method for privacy-preserving distributed training of machine learning models on distributed datasets, 2021
  Patent no: WO/2021/223873

- Sinem Sav, Juan Ramón Troncoso-Pastoriza, Apostolos Pyrgelis, David Froelicher, Joao André Gomes de Sá e Sousa, Jean-Philippe Bossuat, Jean-Pierre Hubaux
  System and method for privacy-preserving distributed training of neural network models on distributed datasets, 2022.
  Patent no: WO/2022/042848

TALKS

- Privacy-Preserving Federated Neural Network Learning for Biomedical Data
  - ❖ Invited talk at 10th International Workshop on Genome Privacy and Security (GenoPri'23), November 2023 (online).
- Privacy-Preserving Federated Neural Network Learning for Disease-Associated Cell Classification
  - ❖ Highlight talk at 27th Annual International Conference on Research in Computational Molecular Biology (RECOMB2023), April 2023, Turkey.
- POSEIDON: Privacy-Preserving Federated Neural Network Learning
  - ❖ CAp2021: Conférence francophone en Apprentissage, June 15, 2021 (online).
  - ❖ Contributed talk for PPML NeurIPS'20, December 11, 2020 (online).
  - ❖ RISELab, UC Berkeley, 2021 (online).
- Privacy-Preserving Federated Learning with Multiparty Homomorphic Encryption
  - ❖ Invited talk at Ozyegin University: IEEE TURKEY Seminar Series, December 22, 2023.
  - ❖ Invited talk at Sabanci University: FENS Graduate Seminar Series, November 8, 2023 (online).
  - ❖ Workshop on Privacy Preserving systems, softwares, and tools at the Department of Mathematics and Physics of the Roma Tre University, October 24, 2022, Italy.
  - ❖ Lecture in Advanced Topics in Computer and Network Security, University of Padua, October 27, 2022, Italy.
  - ❖ Contributed talk and invited panelist at the 3rd International Workshop "Towards Auditable AI Systems: From Use Cases to Standardization & Regulation", November 24, 2022, Germany.

SERVICE

Program Committee Membership: ACNS 2023, ISMB/ECCB 2024, RECOMB PRIEQ 2024.
Reviewer/Ad hoc reviewer: IEEE Transactions on Emerging Topics in Computing, PLOS Computational Biology, PoPETS, USENIX Security, IET Information Security, BMC Medical Informatics, Computers & Security, ISMB/ECCB 2023.

STUDENT SUPERVISION

- Natalija Mitic (Ongoing), Master semester project (12 ECTS), Fall 2022.
- Francesco Intoci (Ongoing), Master semester project (12 ECTS), Spring 2022.
- Abdulrahman Diaa, Privacy-Preserving Federated Recurrent Neural Networks, Summer@EPFL, 2021.
- Xavier Oliva I Jurgens, Privacy-Preserving Federated Hyperparameter Tuning on Non-IID Data Silos: A Measurement Study, Master semester project (12 ECTS), Fall 2021.
- Shufan Wang, Privacy-Preserving Federated Neural Network Training for Disease Associated Cell Detection, Master semester project (12 ECTS), Spring 2021.

- Simon Nicolas Perriard, Privacy-Preserving Hyperparameter Tuning in Federated Learning Setting, Master semester project (12 ECTS), Spring 2021.
- Raphaël Reis Nunes, Distributed Learning with Neural Networks: a performance analysis under decentralization and server failure constrains, Bachelor semester project (8 ECTS), Spring 2020.
- Claire Marie Louise Lefrancq, Convolutional Neural Networks for Disease-Associated Cell Detection, Bachelor semester project (8 ECTS), Fall 2020.

HONORS & AWARDS

- 1st prize for the paper "POSEIDON: Privacy-Preserving Federated Neural Network Learning " in CSAW'21 Applied Research Competition (Prize: 700€).
- 2nd place for the "Homomorphic Encryption-based Secure Viral Strain Classification", iDASH21.
- Awarded with tuition waiver for Mitacs Globalink Programme, Canada.
- Awarded with tuition waiver from Bilkent University due to high ranking in University Entrance Exam.
- Bilkent University, Senior Design Project, the Best Demonstration Award.