MERT YASSI

PERSONAL DETAILS

E-mail   : mert.yassi@monash.edu
LinkedIn Address : linkedin.com/in/mert-yassi
GitHub Address   : github.com/yassimert
ORCID ID   : https://orcid.org/0000-0001-7328-950

EDUCATION

Jul. 2023 – …	Ph.D. in Information Technology, *Monash University,* Melbourne, Australia FIT Research Scholarship, FIT International Postgraduate Research Scholarship
Jul. 2019 – Aug. 2022	Master's Degree, Computer Engineering, *Yasar University*, Izmir, Turkey Full Scholarship, GPA: 3.91/4.00
Sep. 2015 – June 2019	Bachelor's Degree, Computer Engineering, *Yasar University*, Izmir, Turkey Full Scholarship, GPA: 3.90/4.00 (Highest Ranked Student)

WORK EXPERIENCE

Aug. 2023 – …	Sessional Teaching Associate, Faculty of I.T., *Monash University*, Melbourne
Oct. 2019 – Jul. 2023	Full-time Research Assistant, Faculty of Engineering, *Yasar University*, Izmir

PROJECTS

Nov. 2023 – Feb. 2024	Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices Our work has been accepted to ACM CCS 2024
Oct. 2018 – May 2019	Bachelor of Science Thesis, *Yasar University,* Izmir A 4-way Implementation of SIDH Compatible Isogeny Evaluations on Kummer Surfaces https://github.com/yassimert/K4SIDH
Oct. 2017 – Feb. 2019	Scientific Research Project, *Yasar University*, Izmir Fast 4-way vectorized ladder for the complete set of Montgomery curves https://eprint.iacr.org/2020/388.pdf

PARTICIPATIONS/TALKS

June 2022	Summer School on Real-World Crypto and Privacy. Šibenik, Croatia
Sept. 2019	Cryptography Workshop, *Izmir Institute of Technology,* Izmir

PUBLICATIONS

Oct. 2024	R. Steinfeld, A. Sakzad, M. Esgin, V. Kuchta, M. Yassi and R. Zhao, "Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices", in ACM CCS 2024, Salt Lake City, U.S.A., 2024 (accepted, to appear)
Jun. 2022	H. Hisil, B. Egrice and M. Yassi, "Fast 4 way vectorized ladder for the complete set of Montgomery curves", *International Journal of Information Security Science*, vol. 11, no. 2, pp. 12-24, Jun. 2022

COMPUTER SKILLS

	C/C++, Java, Magma Computer Algebra System, SageMath, Python, x64 Assembly, SQL, LaTeX