

Mohamad Mansouri, Ph.D.

 <http://m-mansouri.com>
 [www.github.com/MohamadMansouri](https://github.com/MohamadMansouri)
 mohamad_mansouri@outlook.com
 Toulouse, France



Summary

- Cryptographer expert in designing and implementing crypto solutions based on best security standards.
- Security researcher experienced in vulnerability analysis for Web 3 and decentralized applications.
- Exhibits excellent problem-solving, project management, writing, and communication skills.

Employment History

- **Web 3 Security Researcher. (2024 – present)** Dedaub, Malta.
 - Performing security audits for decentralized protocols.
 - Designing novel security solutions for blockchain technology.
- **Senior Cryptography Software Engineer. (2023 – 2024)** NXP Semiconductors, France.
 - Developing and maintaining cryptography libraries for NXP products.
 - Hardening of NXP crypto libraries against fault attacks and side channel attacks.
- **Security Research Engineer. (2020 – 2023)** Thales SIX GTS, France.
 - Researching and developing new security protocols for privacy protection.
 - Integrating research results into Thales products.
- **Final Year Internship. (2019)** Stevens Institution of Technology, USA.
 - Researching automatic patching and remediation techniques
- **Summer Internship. (2018)** Digital Security Department, EURECOM, France.
 - Researching privacy-preserving techniques for machine learning
- **Penetration Tester. (2017)** NetRom Consultants, Lebanon.
 - Performing black-box penetration testing for web applications and internal networks.

Education

- **Ph.D., University of Sorbonne. (2020 – 2023)** *Cryptography and Security.*
- **Engineering Diploma, Telecom ParisTech (EURECOM). (2017 – 2019)** Digital Security.
- **Engineering Diploma, Lebanese University. (2013 – 2017)** Telecommunication and Electronics.

Skills

Cryptography	■	NIST and ISO/IEC Standards, AES, ECC, RSA, PQC, Zero-Knowledge Proofs.
Programming	■	Embedded C, C++, Python, Solidity, Java, Go, Assembly (Arm, RISC V).
Code Auditing	■	Smart Contracts, Decentralized Apps, Web Apps, Android Apps
Reverse Engineering	■	IDA Pro, Radare2, Intel Pin, Frida.
Team Tools	■	Jira, Bamboo, BitBucket, Git, Svn, Jenkins, Collabnet.
Languages	■	English (Professional), French (Intermediate), Arabic (Native).
Soft Skills	■	Agile, Communication, Presentation, Critical Thinking, Project Management.

Research Publications

- 1 **Mansouri, M.** (2023). *Performance and Verifiability of IoT Security Protocols* (Theses, Thèses de Sorbonne Université). Retrieved from <https://hal.science/tel-04116533>
- 2 **Mansouri, M.**, Önen, M., Ben Jaballah, W., & Conti, M. (2023). Sok: Secure aggregation based on cryptographic schemes for federated learning. In IACR (Ed.), *Pets 2023, 23rd privacy enhancing technologies symposium, 10-15 july 2023, lausanne, switzerland (hybrid conference)*. IACR, Lausanne.
- 3 **Mansouri, M.**, Xu, J., & Portokalidis, G. (2023). Eliminating vulnerabilities by disabling unwanted functionality in binary programs. In *Proceedings of the 2023 acm asia conference on computer and communications security* (pp. 259–273). [doi:10.1145/3579856.3595796](https://doi.org/10.1145/3579856.3595796)
- 4 **Mansouri, M.**, Önen, M., & Ben Jaballah, W. (2022). Learning from failures: Secure and fault-tolerant aggregation for federated learning. In *Proceedings of the 38th annual computer security applications conference* (pp. 146–158). [doi:10.1145/3564625.3568135](https://doi.org/10.1145/3564625.3568135)
- 5 Marcelli, A., Graziano, M., Ugarte-Pedrero, X., Fratantonio, Y., **Mansouri, M.**, & Balzarotti, D. (2022). How machine learning is solving the binary function similarity problem. In Usenix (Ed.), *Usenix 2022, 31st unix security symposium, 10-12 august 2022, boston, ma, usa*, Boston. Retrieved from <https://www.usenix.org/conference/usenixsecurity22/presentation/marcelli>
- 6 **Mansouri, M.**, Ben Jaballah, W., Önen, M., Rabbani, M. M., & Conti, M. (2021). Fadia: Fairness-driven collaborative remote attestation. In *Proceedings of the 14th acm conference on security and privacy in wireless and mobile networks* (pp. 60–71). [doi:10.1145/3448300.3468284](https://doi.org/10.1145/3448300.3468284)
- 7 **Mansouri, M.**, Bozdemir, B., Önen, M., & Ermis, O. (2020). Pac: Privacy-preserving arrhythmia classification with neural networks. In A. Benzekri, M. Barbeau, G. Gong, R. Laborde, & J. Garcia-Alfaro (Eds.), *Foundations and practice of security* (pp. 3–19). [doi:10.1007/978-3-030-45371-8_1](https://doi.org/10.1007/978-3-030-45371-8_1)