Iraklis Leontiadis

Cryptography, Information Security, Engineering

10 years academia, 9+ years industry

Lived, worked and studied in Greece, France, USA and Switzerland

☎ *https://github.com/leontiad*
https://github.com/leontiadZen
✉ *leontiad_a_t_ gmail.com*
leontiad.github.io/

Tech Stack

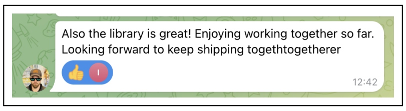
- Rust,C++, Python
- github workflows, Dockers

Talks

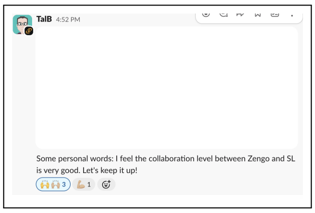
- Digital Asset Debate: Busting myths. Decompute 2024
- Deploying 2 Party ECDSA Signatures in the wild. Open Source Cryptography Workshop 2024, co-located with Real World Cryptography 2024, invitation by Google.
- Namada and Private Bridges. Cosmoverse 2022. Interchain Travel
- Bosch RTC, Pittsburgh, USA, August 2016
- AtheCrypto, Athens, Greece, 2015
- Network and Security Seminar - Eurecom, Sophia Antipolis, France, March 2015
- Inria, Paris-Rocquencourt, 2012

Employment - References upon request

Feb 2024 - now **Head Security Architect**, *Silence labs*, https://www.silencelaboratories.com

- Lead security of product in numerous endpoints
- Manage a team of cryptography and security engineers
- Actively contributing to rust codebase and leading reviews in all repos.
- Architecting multiplatform mobile SDK
- Wells Fargo Custodial lead
- BitGo Custodial/Migration lead
- Thor-Vultisig dkls/schnorr migration lead
- 

  Also the library is great! Enjoying working together so far. Looking forward to keep shipping togethtogetherer

  12:42
- ZenGo Eddsa/Dkls Migration lead
- 

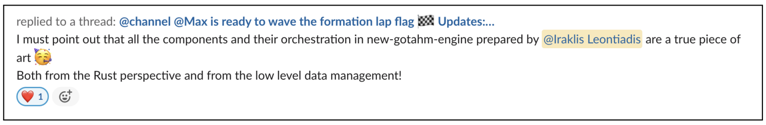
  TalB 4:52 PM

  Some personal words: I feel the collaboration level between Zengo and SL is very good. Let's keep it up!

  🙌🙌 3 💪 1
- Design, Architect and cryptography audits

December 2022 - Jan 2024

Head of Cryptography, *ZenGo Wallet*, https://www.zengo.com

- Research and Development of threshold signatures
- Maintain https://github.com/ZenGo-X
- Rebuilt gotham with a new engine, explained here.
- 
  replied to a thread: @channel @Max is ready to wave the formation lap flag 🏁 Updates:...
  I must point out that all the components and their orchestration in new-gotahm-engine prepared by @Iraklis Leontiadis are a true piece of art 🥳
  Both from the Rust perspective and from the low level data management!
  ❤️ 1
- Security audits
- Lead Security features Roadmap - Lead a team of 2
- Production level code for devops,app,tests,deploy: github CI/CD, AWS
- Full pipeline PoCs for MPC wallets in rust,nodejs and testnets Goerli through ether-rs
- Coordinate and mitigate vuln reports: Certik, Fireblocks :
- C-level meetings for strategic product decisions
- Implement internally https://slsa.dev/
- Security advocate for the company

June 2022 - Dec 22

Lead Cryptographer, *https://anoma.net*

- Design a private bridge for anoma network
- Design a secure wallet for anoma
- Audit code: ics23 standard and Merklee proofs

Oct 2021 - May 2022

Head of Research, *https://www.parfin.io*

- Lead/implement the research roadmap
- Manage a team of 4
- Cryptography and security audits of the codebase
- Integrate MPC threshold signature solution to product
- Client facing and POCs
- Execute SOC2 compliance framework

May 2021 - Feb 2022

Crypto/Security/Smart Contract Auditor

- `TerraSwap BLP`
- `SifChain cryptography audit`

March 2019-October 2021

Senior Cryptography/Security Research Engineer, *Inpher*, Lausanne, Switzerland - Acquired by Arcium

Accomplishments:

- Production level code for XOR-Crypto-MPC-Engine v2 (C++17, 35k LOC)
- Design, implementation, testing, deployment, integration for key agreement and end-to-end encryption for the MPC players.
- Build Privacy Preserving ML solutiong on top of XOR-MPC: linear/logistic regression, similarity detection, XG-Boost
- Benchmarking RAM, Network, CPU for Xor-Engine
- Guideline the security of the entire product
- Formal Security Analysis of XOR-Engine v2
- Technical Leader for H2020 Moore4Medical WP6 in Secure Computing
- Collaborating with external Academic Community, Directors and Managers
- Regular meetings with CTO/CEO/Executives internally.

Oct 2017–Feb 2019

Senior Researcher, *EPFL*, Computer Science, LASEC Group, Lausanne, Switzerland

Supervisor: Prof. Serge Vaudenay, LASEC Lab Director at EPFL.

Scientific Results:

- Iraklis Leontiadis, Serge Vaudenay *Private Message Franking* (submitted)
- Iraklis Leontiadis, Lois Huguenin-Dumittan *A Message Franking Channel* (submitted)

Oct 2016–Oct 2017

Postdoctoral Research Associate, *New Jersey Institute of Technology*, Computer Science, NJ, USA

Supervisor: Prof. Reza Curtmola, Cybersecurity Research Center co-director at NJIT.

Scientific Results:

- Iraklis Leontiadis, Reza Cutmola *Auditable Compressed Storage*, **ISC** 2019 NY, USA 2019.
- Iraklis Leontiadis, Reza Cutmola *Secure Storage with Replication and Transparent Deduplication*, **CODASPY** 2018 Tempe, Arizona, USA 2018.

Oct 2015–Oct 2016 **Postdoctoral Research Associate**, *Univerity of Arizona*, Electrical and Computer Engineering, Tucson, USA

Supervisor: Prof. Ming (Fred) Li, Wiser Lab Director at UofA.

Scientific Results:

- Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li, and Yuqing Zhang *SecuReach: Compute Reachability over Encrypted Data.* In Proceedings of the 15th International Conference on Cryptology and Network Security **CANS 2016**, Milano, Italy, November 2016.
- Iraklis Leontiadis, Ming Li *Substring Searchable Symmetric Encryption Revised*, **ASIACCS-SCC** 2018 Incheon, Korea 2018.
- Hanyu Quan, Boyang Wang, Ming Li, Iraklis Leontiadis and Yuqing Zhang *Efficient and Secure Reachability Computation on Encrypted Location Data* (pending major revision IEEE TCC)
- Iraklis Leontiadis, Ming Li *Collusion Resistant Aggregation from Convertible Tags.* International Journal of Information Security (**IJIS 2020**)

2009–2011 **Research Engineer**, *Inria*, Arles team, Paris-Rocquencourt, France

Supervisor: Dr. Animesh Pathak

Accomplishments:

- An application development toolkit for the Internet of Things, `http://code.google.com/p/srijan-toolkit/`
- An ontology parser for mobile social applications, `https://bitbucket.org/leontiad/yarta`

2006–2007 **Senior Software Engineer**, *Velti S.A*, Mobile Value Added Services Department, Greece

I was part of a 5 members team. I implemented various applications in Java. I was also involved in the configuration and installation of Kannel SMS gateway; which is responsible for receiving SMS's in an application server and then the SMS's were parsed appropriately depending the content and the SMS contest.

Education

2011–2015 **Ph.D. in Computer Science**, *Ecole Nationale Superieure des Telecommunications, Security Protocols and Applied Cryptography group, EURECOM*, France, **Thesis supervisor**: Prof. Refik Molva

Title: Privacy Preserving Data Collection and Analysis

2007–2009 **M.Sc. in Computer Science**, *Athens University of Economics and Business*, Greece

Major: Anonymizing the SIP protocol

2002–2006 **B.Sc. in Computer Science**, *University of Crete*, Greece

Academic experience

Publications

1. Iraklis Leontiadis, Serge Vaudenay: *Private Message Franking.* **ICICS 2023**
2. Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li: FastReach: A System for Privacy-Preserving Reachability Queries over Location Data. **Journal of Computers and Security 2023**
3. M.G. Belorgey, S. Carpov, K. Deforth, N. Gama, D. Jetchev, J. Katz, I. Leontiadis, M. Mohammadi, A. Sae-Tang, M. Vuille: *Manticore: Efficient and Scalable Secure Multiparty Computation.* **International Journal of Cryptology 2023**
4. Iraklis Leontiadis, Lois Huguenin-Dumittan *A Message Franking Channel*, **Inscrypt 2021, Shandong, China**
5. Iraklis Leontiadis, Ming Li *Collusion Resistant Aggregation from Convertible Tags.* **International Journal of Information Security 2020**
6. Iraklis Leontiadis, Reza Cutmola *Auditable Compressed Storage*, **ISC 2019** NY, USA 2019.
7. Iraklis Leontiadis, Ming Li *Substring Searchable Symmetric Encryption Revised*, **ASIACCS-SCC 2018** Incheon, Korea 2018.
8. Iraklis Leontiadis, Reza Cutmola *Secure Storage with Replication and Transparent Deduplication*, **CODASPY 2018** Tempe, Arizona, USA 2018.
9. Hanyu Quan, Boyang Wang, Iraklis Leontiadis, Ming Li, and Yuqing Zhang *SecuReach: Compute Reachability over Encrypted Data.* In Proceedings of the 15th International Conference on Cryptology and Network Security **CANS 2016**, Milano, Italy, November 2016.
10. Iraklis Leontiadis, Kaoutar Elkhiyaoui, Melek Önen, Refik Molva. *PUDA–Privacy and Unforgeability for Data Aggregation.* In Proceedings of the 14th International Conference on Cryptology and Network Security **CANS 2015**, Marrakesh, Morocco, December 2015.
11. Iraklis Leontiadis, Kaoutar Elkhiyaoui, Refik Molva. *Private and Dynamic Time-Series Data Aggregation with Trust Relaxation.* In Proceedings of the 13th International Conference on Cryptology and Network Security **CANS 2014**, Heraklion, Crete, Greece, October 2014.
12. Iraklis Leontiadis, Refik Molva, Melek Önen. *Privacy Preserving Statistics in the Smart Grid.* In Proceedings of the 13th International Workshop on Big Analytics for Security, in conjunction with **ICDCS 2014**, Madrid, Spain, June 2014
13. Iraklis Leontiadis, Refik Molva, Melek Önen. *A P2P Based Usage Control Enforcement Scheme Resilient to Re-injection Attacks.* In Proceedings of the Fifteenth International Symposium on a World of Wireless, Mobile and Multimedia Networks **WoWMoM 2014**, Sydney, Australia, June 2014
14. Iraklis Leontiadis, Melek Önen, Refik Molva, M.J. Chorley, G.B. Colombo. *Privacy preserving similarity detection for data analysis.* In Proceedings of the Collective Social Awareness and Relevance Workshop 2013, co-located with the Third International Conference on Cloud and Green Computing. Karlsruhe, Germany, September 2013
15. Iraklis Leontiadis, Constantinos Delakouridis, Leonidas Kazatzopoulos, Giannis F. Marias. *ANOSIP: Anonymizing the SIP protocol.* In Proceedings of the Measurement, Privacy and Mobility Workshop, co-located with **EuroSys 2012**. Bern, Switzerland, April 2012

Other

- *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value.* World Economic Forum, White paper, Committed to improving the state of the World, September 2019, https://bit.ly/2kg0KoZ
- *Startup holds 'secret' to analyzing private data without accessing it.* EPFL News, April 2019, https://bit.ly/32e8Mzw
- *The Role of Signatures in Digital Assets and Cryptocurrencies* https://medium.com/the-parfin-blog/the-role-of-signatures-in-digital-assets-and-cryptocurrencies-8c242195e
- *One Engine many Championships* https://zengo.com/one-engine-many-championships/

Contribution to National European/Swiss/USA Projects

- H2020-ECSEL Moore4Medical (PI)
- CTI BIOID, 2017-2018, Switzerland.
- NSF Secure and Reliable Outsourced Storage Systems Using Remote Data Checking. 2016-2017, U.S.A.
- FP7 User Centric Networking. 2013-2016, Europe.

Teaching

- Special topics on Applied Cryptography, NJIT, Fall 2016
- 2h Introductory Seminar on Cryptography, ECE University of Arizona, Spring 2015
- Secure communications, M.Sc in Communications and Computer Security, Ecole Nationale Superieure des Telecommunications, Fall 2012, 2013, 2014
- Secure applications in networking and distributed systems, M.Sc in Communications and Computer Security, Ecole Nationale Superieure des Telecommunications, Spring 2012, 2013, 2014

Supervisory

- Andrea Caforio, *The DUHK-Attack.* (Seminar supervision Spring 2018 - EPFL)
- Vadim Vadydov, *KRACK attack (802.11i four-way handshake attack).* (Seminar supervision Spring 2018 - EPFL)
- Anshul Anand, *A secure storage protocol.* (Summer 2018 Intern at EPFL - Supervision)
- Lois Huguenin-Dumittan, *Message Franking in real world.* (Master Student at EPFL, Semester project 2017-2018 supervision)
- Hanyu Quan, Ph.D. student in Cyptography, Xidian University. Mentoring at University of Arizona Oct 2015 - ongoing.
- Lorenzo David. *Private and Dynamic Computations for single board computers.* (Spring Semester 2015)
- Stevan Vuviv, Nikhil Gupta, Abbas Hassoun. *Private and Dynamic Data Analysis.* (Fall-Spring Semester-Project 2015)
- Cédric Van Rompey. *Multi User Keyword Search With Small Leakages.* (Eurecom Internship-Spring Semester 2014)
- Anna Kozachenko. *Secure Usage Control Enforcement based on a P2P network.* (Master project-Spring semester 2013
- Cesar Burini, Guillaume Gruber. *Accountability for the Cloud.* (Master project-Fall semester 2012)

Services

- Organisation: Session Chair: ML and Security, ISC 2019
- Steering Committee: DeCompute 2024
- TPC member for: ASIAPKC 2018-24, ICC 2018, ICISC 2019-24
- Shadow PC Eurosys 2016, 2017
- External scientific reviewer for the following conferences: IEEE Future Network and Mobile-Summit 2010, ACM WiSec 2012, ACNS 2012, CANS 2012, FC 2013, CCS 2013, CRISIS 2013, INFOCOM 2014, NDSS 2014, ICC 2014, CNS 2014, CCS 2014, INFOCOM 2016, ASIACCS 2016, CANS 2016, FC 2017, CNS 2017, ESORICS 2017, ASIACRYPT 17, CANS 17, CCSW 17, PKC 18, ACISP 18, ASIACCS-SCC 18, ESORICS 18, ASIACRYPT 18, INDOCRYPT 18, INFOCOM 2019.
- Reviewer for the following journals: Elsevier Computer Communications, International Journal of Information Security, Transactions on Information Forensics and Security, ACM Transactions on Sensor Networking, IEEE Transactions on Dependable and Secure Computing, Elsevier Computers and Security, ACM Transactions on Privacy and Security (TOPS).

Languages

- Greek Native
- English Fluent
- French Good