Panagiotis Chatzigiannis

Curriculum Vitae

Fairfax, VA
United States
703-679-7019
pchatzig@gmu.edu
https://panoschtz.github.io

Research Interests

Cryptography and Blockchains - privacy, auditability/accountability, recovery and key management for blockchains and decentralized payments

Education

August 2017 - June 2022 **PhD Student in Computer Science**, *George Mason University*, Fairfax, VA, GPA:3.92.
Advisor: Prof. Foteini Baldimtsi

2010 - 2012 **MSc. Computer Science**, *Naval Postgraduate School*, Monterey, CA, GPA:3.82.
Thesis Topic: *Connecting Land-based Networks to Ships*
Advisers: Prof. Gurminder Singh, John H Gibson

1997 - 2001 **BSc. Engineering**, *Hellenic Naval Academy*, Piraeus, Greece.

Work Experience and Internships

June 2022 - present **Visa Research** , *Research Scientist*.

May 2021 - Sep 2021 **Facebook (Diem)** , *Summer intern*.
- Light client systematization of knowledge - techniques towards building light clients applicable to blockchain systems as Diem
- Preliminary work towards compressing various cryptographic primitives through brute-force process

May 2020 - Dec 2020 **Facebook (Diem)** , *Summer intern and Part-Time Student Researcher* .
- Diem Proof of Assets protocol enhancing regulatory compliance of Diem's product
- Methods for compressing small discrete-log lookup tables by a factor of 10 without additional computational costs

2001 - 2017 **Greek Navy**, *Lieutenant Commander*.
- Chief engineer and electronics officer on Submarines/Frigates
- IT Director in Technical Department of Souda Naval Base
- IT officer in NATO Maritime Interdiction Operational Training Centre
- Naval Cyber-defense and incident response team member

Teaching Assistantships - Research Assistantships

Summer 2018 - Present **Research Assistant**.

Fall 2017 - Spring 2018 **Teaching Assistant**.

- Network Security
- Computer Architecture
- Introduction to Computer Programming

Publications

- **P. Chatzigiannis**, F. Baldimtsi, I. Griva, J. Li, "Diversification across pools: Optimal mining strategies under PoW", *WEIS 2019*.
- **P. Chatzigiannis**, F. Baldimtsi, C. Kolias and A. Stavrou, "Black-Box IoT: Authentication and Distributed Storage of IoT Data from Constrained Sensors", *IoTDI 2021* (acceptance rate 25%).
- **P. Chatzigiannis**, F. Baldimtsi, "MiniLedger: Compact-sized Anonymous and Auditable Distributed Payments", *ESORICS 2021* (acceptance rate 20%).
- **P. Chatzigiannis**, F. Baldimtsi and K. Chalkias, "SoK: Auditability and Accountability in Distributed Payment Systems", *ACNS 2021* (acceptance rate 20%).
- **P. Chatzigiannis**, K. Chalkias, "Proof of Assets in the Diem Blockchain", *AIBlock 2021*.
- **P. Chatzigiannis**, K. Chalkias, V. Nikolaenko, "Homomorphic decryption in blockchains via compressed discrete-log lookup tables", *CBT 2021*.
- S. Blackshear, K. Chalkias, **P. Chatzigiannis**, R. Faizullabhoy, I. Khaburzaniya, E. Kokoris Kogias, J. Lind, D. Wong, T. Zakian, "Reactive Key-Loss Protection in Blockchains", *WTSC 2021*.
- **P. Chatzigiannis**, F. Baldimtsi and K. Chalkias, "SoK: Blockchain Light Clients", *FC 2022*.
- K. Chalkias, **P. Chatzigiannis**, and Y. Ji, "Broken Proofs of Solvency in Blockchain Custodial Wallets and Exchanges".
- F. Baldimtsi, **P. Chatzigiannis**, S. Dov Gordon, P. Hung Le, D. McVicker, "gOTzilla: Efficient Disjunctive Zero-Knowledge Proofs from MPC in the Head, with Application to Proofs of Assets in Cryptocurrencies", *PETS 2022*.
- ***P. Chatzigiannis**, L. K. L. Ng, D. V. Le, M. Minaei, R. Kumaresan, M. Zamani (2024). "A Plug-and-Play Long-Range Defense System for Proof-of-Stake Blockchains".*
- *M. Minaei, **P. Chatzigiannis**, S. Jin, S. Raghuraman, R. Kumaresan, M. Zamani, P. Moreno-Sanchez (2023). "Unlinkability and Interoperability in Account-Based Universal Payment Channels",* Financial Cryptography and Data Security. FC 2023 International Workshops.
- ***P. Chatzigiannis**, W. C. Gu, S. Raghuraman, P. Rindal, M. Zamani (2023). "Privacy-Enhancing Technologies for Financial Data Sharing".*
- *S. S. Arora, A. Beams, **P. Chatzigiannis**, S. Meiser, K. Patel, S. Raghuraman, P. Rindal, H. Shah, Y. Wang, Y. Wu, H. Yang, M. Zamani (2023). "Privacy-Preserving Financial Anomaly Detection via Federated Learning & Multi-Party Computation",* 2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops).
- M. Minaei, **P. Chatzigiannis**, S. Jin, S. Raghuraman, R. Kumaresan, M. Zamani, P. Moreno-Sanchez (2023). "Unlinkability and Interoperability in Account-Based Universal Payment Channels".
- **P. Chatzigiannis**, K. Chalkias, A. Kate, E. V. Mangipudi, M. Minaei, M. Mondal (2023). "SoK: Web3 Recovery Mechanisms".
- F. Baldimtsi, K. Chalkias, **P. Chatzigiannis**, M. Kelkar (2023). "Truncator: Time-space Tradeoff of Cryptographic Primitives", *FC 2024*.
- *L. K. L. Ng, **P. Chatzigiannis**, D.V. Le, M. Minaei, R. Kumaresan, M. Zamani (2024). "A Plug-and-Play Long-Range Defense System for Proof-of-Stake Blockchains",* ESORICS 2024.
- D. Aronoff, A. Bhat, **P. Chatzigiannis**, M. Minaei, S. Raghuraman, R.M. Townsend, N. X. Y. Zhang (2025). "SoK: Fully-homomorphic encryption in smart contracts".
- M. Minaei, P. Moreno-Sanchez, Z. Fang, S. Raghuraman, N. Alamati, **P. Chatzigiannis**, R. Kumaresan, D.V. Le, (2025). "DTL: Data Tumbling Layer - A Composable Unlinkability for Smart Contracts" (AsiaCCS 2025).

- L. KL Ng, P. Moreno-Sanchez, M. Minaei, **P. Chatzigiannis**, A. Bhat, D.V. Le, (2025). "Lite-PoT: Practical Powers-of-Tau Setup Ceremony" (CCS 2025).
- **P. Chatzigiannis**, C. Wang, M. Minaei, S. Arora (2025). A Composability Analysis Framework for Web3 Wallet Recovery Mechanisms" (IEEE S&P 2025).
- M. Minaei, D. V. Le, R. Kumaresan, A. Beams, P. Moreno-Sanchez, Y. Yang, S. Raghuraman, **P. Chatzigiannis**, M. Zamani. "Scalable Off-Chain Auctions" (NDSS 2026).
- P. Moreno-Sanchez, M. Minaei, S. Raghuraman, **P. Chatzigiannis**, D. V. Le. "AUPCH: Auditable Unlinkable Payment Channel Hubs" (CBT 2026).
- **P. Chatzigiannis**, K. Chalkias, A. Kate, E. V. Mangipudi, M. Minaei, M. Mondal (2025). "Web3 Recovery Mechanisms and User Preferences".
- **P. Chatzigiannis**, S. Chakraborty, S. Ahmed (2025). "LifeXP: Secure, usable and reliable key recovery for Web3 applications" (available upon request).

Additional Presentations and Invited Talks

- "Mimblewimble: a blockchain design with no script support and blinded amounts", *GMU Crypto and Security Reading Group, February 2018*
- "Accountable Privacy in Distributed Payment Schemes", *George Mason University, May 2019*
- "MiniLedger: A Compact-sized Anonymous and Auditable Distributed Payment Scheme", *Facebook/Novi 1st Novice Seminar, June 2020*.
- "Novi Proof of Assets", *Facebook/Novi 6th Novice Seminar, September 2020*.
- "Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings", *GMU Crypto and Security Reading Group, October 2020*.
- "MiniLedger: Compact-sized Anonymous and Auditable Distributed Payments", *Cornell University Security Seminar, November 2020*.
- "MiniLedger: A Compact-sized Anonymous and Auditable Distributed Payment Scheme", *Athecrypt 2021*.

Program Committees

- PETS 2023
- Financial Cryptography 2023
- PETS 2024 Artifact committee
- Financial Cryptography 2024
- PETS 2025
- PETS 2025 Artifact committee
- Financial Cryptography 2025
- IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2025
- PETS 2026
- PETS 2026 Artifact committee
- Financial Cryptography 2026
- CCS 2026

Conferences - Workshops attended

- IACR Summer School - Blockchain Technologies 2016 (Corfu, Greece)
- DIMACS 2017 (Rutgers University) - received travel grant
- Scaling Bitcoin 2017 (Stanford University) - received travel grant
- DC Area Crypto Day December 2018 (University of Maryland)
- DC Area Crypto Day April 2019 (NIST)
- Real World Crypto 2020 (Columbia University) - received travel grant

- ZKProof workshop 2020 (Virtual)
- ZKProof workshop 2021 (Virtual)
- Financial cryptography 2021 (Virtual)
- Advances in Financial Technologies (AFT) 2021
- SBC 2022
- SBC 2023
- ZKProof DC 2023
- Crypto Council for Innovation 2024
- Crypto Council for Innovation 2025
- PGP* for Crypto Events 2025

Conferences external reviewer

- 2018 International Cryptology Conference
- 4th Smart Cloud Networks & Systems Conference 2018
- 25th ACM Conference on Computer and Communications Security 2018
- IEEE Systems, Man and Cybernetics: Systems (Blockchain) 2018
- 2019 Network and Distributed System Security Symposium (NDSS)
- Financial Cryptography 2019
- 40th IEEE Symposium on Security and Privacy 2019
- 22nd Information Security Conference 2019
- IEEE 2019 Crypto Valley Conference
- Advances in Financial Technologies (AFT) 2019
- Financial Cryptography 2020
- ACM CCS 2020
- Financial Cryptography 2021
- Eurocrypt 2021
- Advances in Financial Technologies (AFT) 2021
- Financial Cryptography 2022
- Eurocrypt 2025

Awards

April 2016 **National Bank of Greece Fintech Hackathon**, *"Loyalty Points" reward tracking on Ethereum smart contracts*.

May 2016 **"Panoptis 2016" National Cyberdefense Exercise**, *Linux Systems Forensics - Navy commendation*.

March 2023 **PETs Challenge 2022**, *Special Recognition Prize*.

Technical Skills

Programming Languages	Python, Rust, C, C++, Java, Go, Arduino, Solidity
Databases - Networking	Oracle, MSSQL, MySQL, Cisco IOS, Wireshark, CNSSI 4013A – System Administrators Certificate

Languages

English, Greek (Native), German