PEDRO MORENO-SANCHEZ

IMDEA Software Institute
pedro.moreno@imdea.org

EARNED DEGREES

Ph.D. 2018 Purdue University Department of Computer Science USA
Thesis: Credit Network Payment Systems: Security, Privacy and Decentralization
Advisor: Aniket Kate

M.S. 2013 University of Murcia Department of Computer Science Spain
Thesis: Multicast Group Security Architecture for Internet of Things
Advisors: Oscar Garcia-Morchon, Sye Keoh, Sandeep Kumar and Rafael Marin-Lopez

B.S. 2011 University of Murcia Department of Computer Science Spain
Thesis: An Open Source Implementation of the Protocol for Carrying Authentication for Network Access
Advisor: Rafael Marin-Lopez

RESEARCH INTERESTS

I am interested in *distributed networked systems*, *information security*, *applied cryptography* and *privacy-enhacing technologies*. My work aims at formalizing and developing cryptographic solutions for secure, privacy-preserving network systems. My current research focuses on the security, privacy, scalability and interoperability of distributed ledgers (or blockchains).

RESEARCH EXPERIENCE

Research Consultant (part time)	VISA Research, Palo Alto (USA)	May 2023 – *present*
Assistant Professor	IMDEA Software Institute, Madrid (Spain)	Oct 2020 – *present*
Postdoc	Technical University of Vienna, Vienna (Austria)	Sep 2018– Sep 2020
Intern	IBM-Zurich Research Labs, Zurich (Switzerland)	Summer 2017
Intern	Ripple Labs, San Francisco (USA)	Summer 2016
Intern	Philips Research Europe, Eindhoven (The Netherlands)	Jun 2012–Dec 2012

TEACHING EXPERIENCE

Lecturer. **Universidad Politecnica de Madrid**

- Design and Analysis of Security Protocols. Graduate level course 2023

Lecturer. **Universidad Autonoma de Madrid**

- Design and Analysis of Security Protocols. Graduate level course 2021, 2022

Lecturer. **Technical University of Vienna**

- Privacy Enhancing Cryptography. Graduate level course 2019, 2020
- Cryptocurrencies. Graduate level course 2019, 2020
- Foundations of Blockchain Technologies. Graduate level seminar 2019

PUBLICATIONS

Hereon, the symbol * denotes that both authors contributed equally and are considered first co-authors.

Hereon, the symbol † denotes that I have given the talk at the conference.

Publications in Top Security and Privacy Conferences.

		2023	2022	2021	2020	2019	2018	2017	2016	2013-2015
1st tier	NDSS	2				1	1	2		1
	CCS	1	3			1		1		
	USENIX Sec			1						
	S&P		1	2						
	WWW						1			
2nd tier	PETS				1			1	1	
	FC	1		3	2					
	ESORICS									1
	ASIACRYPT			1						

Conference Presentation with Proceedings (Refereed)

1. Lukas Aumayr, Esra Ceylan, Yannik Kopyciok, Matteo Maffei, Pedro Moreno-Sanchez, Iosif Salem, Stefan Schmid. *Optimizing Virtual Payment Channel Establishment in the Face of On-Path Adversaries.* In IFIP Networking Conference (IFIP Networking), 2024.

2. Erkan Tairi, Pedro Moreno-Sanchez, Clara Schneidewind. *LedgerLocks: A Security Framework for Blockchain Protocols Based on Adaptor Signatures.* In Computer and Communication Security (CCS), 2023.

3. Oguzhan Ersoy, Pedro Moreno-Sanchez, Stefanie Roos. *Get Me out of This Payment! Bailout: An HTLC Re-routing Protocol.* In Financial Cryptography and Data Security (FC), 2023

4. Varun Madathil, Sri AravindaKrishnan Thyagarajan, Dimitrios Vasilopoulos, Lloyd Fournier, Giulio Malavolta, Pedro Moreno-Sanchez. *Cryptographic Oracle-Based Conditional Payments.* In Network and Distributed System Security Symposium (NDSS), 2023.

5. Lukas Aumayr, Pedro Moreno-Sanchez, Aniket Kate and Matteo Maffei. *Breaking and Fixing Virtual Channels: Domino Attack and Donner.* In Network and Distributed System Security Symposium (NDSS), 2023.

6. Gibran Gomez, Pedro Moreno-Sanchez and Juan Caballero. *Watch Your Back: Identifying Cybercrime Financial Relationships in Bitcoin through Back-and-Forth Exploration.* In Computer and Communication Security (CCS), 2022.

7. Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, Erkan Tairi and Sri Aravinda Krishnan Thyagarajan. *Foundations of Coin Mixing Services.* In Computer and Communication Security (CCS), 2022.

8. Lukas Aumayr and Sri Aravinda Krishnan Thyagarajan and Giulio Malavolta and Pedro Moreno-Sanchez and Matteo Maffei. *Sleepy Channels: Bitcoin-Compatible Bi-directional Payment Channels without Watchtowers.* In Computer and Communication Security (CCS), 2022.

9. Rainer Stütz, Johann Stockinger, Pedro Moreno-Sanchez, Bernhard Haslhofer and Matteo Maffei. *Adoption and Actual Privacy of Decentralized CoinJoin Implementations in the Bitcoin Ecosystem.* In Advances of Financial Technologies (AFT), 2022.

10. Sri Aravinda Krishnan Thyagarajan, Giulio Malavolta and Pedro Moreno-Sanchez. *Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains.* In IEEE Symposium on Security and Privacy (S&P), 2022.

11. Lukas Aumayr, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostakova, Matteo Maffei, Pedro Moreno-Sanchez and Siavash Riahi. *Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures.* In Asiacrypt, 2021.

12. Erkan Tairi, Pedro Moreno-Sanchez and Matteo Maffei. *A2L: Anonymous Atomic Locks for Scalability and Interoperability in Payment Channel Hubs.* In IEEE Symposium on Security and Privacy (S&P), 2021.

13. Lukas Aumayr, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostakova, Matteo Maffei, Pedro Moreno-Sanchez and Siavash Riahi. *Bitcoin-Compatible Virtual Channels.* In IEEE Symposium on Security and Privacy (S&P), 2021.

14. Lukas Aumayr, Pedro Moreno-Sanchez, Aniket Kate and Matteo Maffei. *Blitz: Secure Multi-Hop Payments Without Two-Phase-Commits.* In USENIX Security (Sec), 2021.

15. Erkan Tairi, Pedro Moreno-Sanchez and Matteo Maffei. *Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments.* In Financial Cryptography and Data Security (FC), 2021.

16. Matteo Romiti, Friedhelm Victor, Pedro Moreno-Sanchez, Peter Sebastian Nordholt, Bernhard Haslhofer and Matteo Maffei. *Cross-Layer Deanonymization Methods in the Lightning Protocol.* In Financial Cryptography and Data Security (FC), 2021.

17. Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias and William J. Knottenbelt. *SoK: Communication Across Distributed Ledgers.* In Financial Cryptography and Data Security (FC), 2021.

18. Mohsen Minaei*, Pedro Moreno-Sanchez* and Aniket Kate. *MoneyMorph: Censorship Resistant Rendezvous using Permissionless Cryptocurrencies.* In Privacy Enhancing Technologies (PETS), 2020.

19. Pedro Moreno-Sanchez†, Randomrun, Duc V. Le, Sarang Noether, Brandon Goodell and Aniket Kate. *DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero.* In Financial Cryptography and Data Security (FC), 2020.

20. Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry and Arthur Gervais. *SoK: Layer-Two Blockchain Protocols.* In Financial Cryptography and Data Security (FC), 2020.

21. Christoph Egger, Pedro Moreno-Sanchez and Matteo Maffei. *Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks.* In Computer and Communication Security (CCS), 2019.

22. Giulio Malavolta*, Pedro Moreno-Sanchez*, Clara Schneidewind, Aniket Kate and Matteo Maffei. *Anonymous Multi-hop Locks for Blockchain Scalability and Interoperability.* In Network and Distributed System Security Symposium (NDSS), 2019.
Finalist of CSAW'19 Applied Research Competition `https://csaw.engineering.nyu.edu/research`

23. Pedro Moreno-Sanchez†, Navin Modi, Raghuvir Songhela, Aniket Kate and Sonia Fahmy. *Mind Your Credit: Assessing the Health of the Ripple Credit Network.* In World Wide Web Conference (WWW), 2018

24. Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate and Ian Goldberg. *Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions.* In Network and Distributed System Security Symposium (NDSS), 2018

25. Giulio Malavolta*, Pedro Moreno-Sanchez*, Aniket Kate, Matteo Maffei and Srivatsan Ravi. *Concurrency and Privacy with Payment-Channel Networks.* In Computer and Communication Security (CCS), 2017

26. Giulio Malavolta*, Pedro Moreno-Sanchez*†, Aniket Kate and Matteo Maffei. *SilentWhispers: Enforcing Security and Privacy in Decentralized Credit Networks.* In Network and Distributed System Security Symposium (NDSS), 2017

27. Tim Ruffing, Pedro Moreno-Sanchez and Aniket Kate. *P2P Mixing and Unlinkable Bitcoin Transactions.* In Network and Distributed System Security Symposium (NDSS), 2017

28. Pedro Moreno-Sanchez†, Tim Ruffing and Aniket Kate. *PathShuffle: Mixing Credit Paths for Anonymous Transactions in Ripple.* In Privacy Enhancing Technologies Symposium (PETS), 2017

29. Pedro Moreno-Sanchez†, Muhammad Bilal Zafar and Aniket Kate. *Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network.* In Privacy Enhancing Technologies Symposium (PETS), 2016

30. Pedro Moreno-Sanchez†, Aniket Kate, Matteo Maffei and Kim Pecina. *Privacy Preserving Payments in Credit Networks.* In Network and Distributed System Security Symposium (NDSS), 2015

31. Tim Ruffing, Pedro Moreno-Sanchez and Aniket Kate. *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin.* In European Symposium on Research in Computer Security (ESORICS), 2014

32. Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar, Pedro Moreno-Sanchez, Francisco Vidal-Meca, and Jan Henrik Ziegeldorf. *Securing the IP-based Internet of Things with HIP and DTLS.* In Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2013

Journal Articles

1. Donghang Lu, Pedro Moreno-Sanchez, Amanuel Zeryihun, Shivam Bajpayi, Sihao Yin, Ken Feldman, Jason Kosofsky, Pramita Mitra and Aniket Kate. *Towards Privacy-Aware Traceability for Automotive Supply-Chains.* In Journal of Transportation Cybersecurity and Privacy (JTCYBER), 2021.

2. Pedro Moreno-Sanchez, Uzair Mahmood and Aniket Kate. *ClearChart: Ensuring Integrity of Consumer Ratings in Online Marketplaces.* In Computers and Security (CoSe) Journal, 2018. Volume 78.

3. Pedro Moreno-Sanchez, Rafa Marin-Lopez and Francisco Vidal-Meca. *An open source implementation of the protocol for carrying authentication for network access.* In IEEE Networks, 2014. Volume 28. Number 2

4. Antonio J. Jara, Pedro Moreno-Sanchez, Antonio F. Skarmeta, Socrates Varakliotis and Peter T. Kirstein. *IPv6 Addressing Proxy: Mapping Native Addressing from Legacy Technologies and Devices to the Internet of Things (IPv6).* In Sensors, 2013, Volume 13. Number 5

5. Pedro Moreno-Sanchez, Rafa Marin Lopez and Antonio F. Skarmeta. *PANATIKI: A Network Access Control Implementation Based on PANA for IoT Devices.* In Sensors 2013. Volume 13. Number 11.

Workshop Papers

1. Stephan Duebler, Pedro Moreno-Sanchez and Clara Schneidewind. *Generalized Swap Graphs for Blockchain Protocols.* In Workshop on Foundations of Computer Security (FCS), 2023.

2. Federico Badaloni, Chrysoula Oikonomou, *Pedro Moreno-Sanchez* and Clara Schneidewind. *BitMLx – Cross-chain Smart Contracts for Bitcoin-style Cryptocurrencies.* In Workshop on Foundations of Computer Security (FCS), 2023.
3. Mohsen Minaei, Panagiotis Chatzigiannis, Shan Jin, Mahdi Zamani, Ranjit Kumaresan, Srinivasan Raghuraman and Pedro Moreno-Sanchez. *Unlinkability and Interoperability in Account-Based Universal Payment Channels.* In Workshop on Trusted Smart Contracts (WTSC), 2023.
4. Philipp Hoenisch, Subhra Mazumdar, Sushmita Ruj and Pedro Moreno-Sanchez. *LightSwap: An Atomic Swap Does Not Require Timeouts At Both Blockchains.* In International Workshop on Cryptocurrencies and Blockchain Technology (CBT), 2022.
5. Sergei Tikhomirov, Pedro Moreno-Sanchez and Matteo Maffei. *A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network.* In IEEE Security & Priavacy on the Blockchain (IEEE S&B), 2020.
6. Christian Cachin, Angelo De Caro, Pedro Moreno-Sanchez†, Bjoern Tackmann and Marko Vukolic. *The Transaction Graph for Modeling Blockchain Semantics.* In Cryptoeconomics Systems Conference (CES), 2020.
7. Donghang Lu, Pedro Moreno-Sanchez, Amanuel Zeryihun, Shivam Bajpayi, Sihao Yin, Ken Feldman, Jason Kosofsky, Pramita Mitra and Aniket Kate. *Reducing Automotive Counterfeiting using Blockchain: Benefits and Challenges.* In Proceedings of IEEE International Conference on Decentralized Applications and Infrastructures (IEEE DAPPCON), 2019.
8. Adithya Bhat, Pedro Moreno-Sanchez and Aniket Kate. *Transitive Network: Tokenless IOU Credit Network in Ethereum.* In Cryptocurrency Implementers' Workshop (CIW). Workshop Associated with Financial Cryptography and Data Security Conference, 2019.
9. Tim Ruffing and Pedro Moreno-Sanchez. *ValueShuffle: Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin.* In BITCOIN Workshop. Workshop Associated with Financial Cryptography and Data Security Conference, 2017.
10. Francisco Vidal-Meca, Jan Henrik Ziegeldorf, Pedro Moreno-Sanchez, Oscar Garcia-Morchon, Sye Loong Keoh and Sandeep Kumar. *HIP Security Architecture for the IP-Based Internet of Things.* In Conference on Advanced Information Networking and Applications Workshops (WAINA), 2013

CURRENT STUDENTS

Full Name	Position	Institute	Time Period	Co-advisor
Jorge Gonzalez Gutierrez	Master	IMDEA	March 2024 - *Present*	
Javier Gomez Martinez	PhD	IMDEA	Jan 2024 - *Present*	
Federico Badaloni	PhD	MPI-SP	Feb 2023 - *Present*	Clara Schneidewind
Alberto del Amo	Master	IMDEA	Feb 2023 - *Present*	
Diego Castejon Molina	PhD	IMDEA	Oct 2021 - *Present*	

PREVIOUS STUDENTS

Full Name	Position	Institute	Time Period	Co-advisor
Dimitrios Vasilopoulos	Postdoc	IMDEA	Jun 2021 - May 2024	
Javier Gomez Martinez	Master	IMDEA	Feb 2023 - Dec 2023	Dario Fiore
Laura Herrero	Intern	IMDEA	Jan 2023 - Jul 2023	Ignacio Cascudo
Ana Marija Eres	Master	IMDEA	Oct 2021 - Jun 2022	
Chrysoula Oikonomou	Intern	IMDEA	Sep 2021 - Feb 2022	Clara Schneidewind
Istvan Andras Seres	Intern	IMDEA	Sep 2021 - Feb 2022	
Marta Centellas	Master	IMDEA	Apr 2021 - Sep 2021	Ignacio Cascudo
Meresa Gebrewahd	Master	IMDEA	Apr 2021 - Sep 2021	
Jakob Abfalter	Master	TU Vienna	Mar 2020 - Mar 2021	Matteo Maffei
Oguzhan Ersoy	Intern	TU Vienna	Oct 2019 - Dec 2019	
Duc V. Le	Intern	TU Vienna	Jun 2019 - Aug 2019	
Sergei Tikhomirov	Intern	TU Vienna	Jun 2019 - Aug 2019	
Lukas Aumayr	PhD	TU Vienna	Sep 2019 – March 2024	Matteo Maffei
Erkan Tairi	PhD	TU Vienna	Oct 2018 – March 2024	Matteo Maffei & Daniel Slamanig

GRANTS, SCHOLARSHIPS AND AWARDS

2023–2027 **ESPADA (Research Team)** A 4-years project from the Spanish Research Agency (AEI) for research projects at Spanish universities or research institutes. Budget €335K.

2022–2024 **PRODIGY (PI)** A 2-years project from the Spanish Research Agency (AEI) for research projects at Spanish universities or research institutes. Budget €520K.

2022–2025 **Juan de la Cierva (PI)** A 3-years project from the Spanish Research Agency (AEI) that targets highly qualified postdoc researchers of any discipline that could contribute to the scientific development of Spain. Budget €98K.

2019-2022 **BLOQUES (Research Team)** A 4-years project from the Spanish Research Agency (AEI) for research projects at Spanish universities or research institutes. Budget €412K.

2019-2022 **SCUM (Research Team)** A 4-years project from the Spanish Research Agency (AEI) for research projects at Spanish universities or research institutes. Budget €302K.

2019–2022 **CoBloX - TenX (PI)** A research grant from industry to study the blockchain interoperability problem in the COMIT Network. Budget €340K.

2018–2020 **Chaincode Labs - Lightning Labs (PI)** A research grant from industry to study the security and privacy issues in the Lightning Network. Budget €140K.

2018–2020 **Lise Meitner Scholarship (PI)** A 2-years scholarship from the Austrian Science Fund (FWF) that targets highly-qualified postdoc researchers of any discipline who could contribute to the scientific development of an Austrian research institution by working at it. Acceptance rate 30%. `https://www.fwf.ac.at/en/research-funding/application/meitner-programme/`

2017 **Emil Stefanov Award.** This award is given to the graduate student in the Computer Science Department of Purdue University who shows the best academic achievements in security.

2017 **CERIAS/Intel Research Scholarship.** A 1-year scholarship from Intel Research Labs that targets graduate students affiliated to Purdue University with outstanding records in their research areas.

INVITED LECTURES/SCIENTIFIC TALKS

I include here the talks other than those at conferences with proceedings.

1. **Keynote: Establishing secure and privacy-preserving blockchain applications through real world cryptography**
   Workshop on Cryptocurrencies and Blockchain Technology, Poland (2024)
2. **Keynote: Establishing secure and privacy-preserving blockchain applications through real world cryptography**
   Workshop on Data Privacy Management, Poland (2024)
3. **My Journey in Security and Privacy in Credit Networks**
   Workshop on Decentralized Credit Networks, USA (2023)
4. **Privacy-preserving Blockchain Applications With Adaptor Signatures**
   Computer Science Hub - Vienna, Austria (2022)
5. **Generalized Channels from Limited Blockchain Scripts and Applications**
   University of Bern, Switzerland (2022)
6. **Keynote: Security and Privacy of Payment Channels and Applications**
   Crypto Valley Conference (CVC), Online (2021)
7. **Panel: Layer 2 Swaps**
   Advances of Financial Technologies (AFT), Online (2021)
8. **Blitz: Secure Multi-Hop Payments Without Two-Phase-Commits**
   Protocol Research Labs, Online (2021)
9. **Security, Privacy and Scalability for Blockchains**
   Cryptography Research Centre, Online (2021)
10. **Universal Atomic Swaps: Fair Exchange of Coins Across All Blockchains**
    Crosschain Communications Workshop, Online (2021)
11. **Security, Privacy and Interoperability in Payment-Channel Hubs**
    BIS: Workshop on Blockchain Interoperability and Sharding, Online (2020)
12. **Security, Privacy and Scalability in Blockchains**
    4th ForDigital Blockchain Workshop, Online (2020)
13. **Challenges and Cryptographic Solutions with Payment-Channel Networks**
    Real World Cryptography, USA (2020)
14. **Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks**
    Scaling Bitcoin, Israel (2019)
15. **A2L: Anonymous Atomic Locks for Scalability and Interoperability in Payment Channel Hubs**
    Scaling Bitcoin, Israel (2019)
16. **Dual Outputs: Enabling Payment-Channel Networks in Monero**
    The Monero Conference, USA (2019)
17. **Privacy-preserving Multi-hop Locks for Blockchain Scalability and Interoperability**
    Stanford Blockchain Conference, USA (2019)

Master Workshop: Off the chain, Germany (2018)
Scaling Bitcoin, Japan (2018)

18. **Security and Privacy Challenges in Path-Based Transaction Networks**
EPFL, Switzerland (2018)
ETH Zurich, Switzerland (2017)
IBM-Research Zurich, Switzerland (2017)

19. **Introduction to Bitcoin**
University of Murcia, Spain (2018)

20. **Concurrency and Privacy with Payment-Channel Networks**
Scaling Bitcoin, USA (2017)

21. **Listening to and Silencing the Whispers of Ripple: Study and Solutions for Privacy in IOweYou Credit Networks**
Real World Cryptography, USA (2017)
George Mason University, USA (2017)
Ripple Labs, USA (2016)

SERVICE

Program Committee (Co-)Chair

- 2025: Financial Cryptography and Data Security
- 2023: Student Support for Network and Distributed System Security Symposium.
- 2021: Conference on Decentralized Applications and Infrastructures, IEEE Workshop on Security & Privacy on the Blockchain.
- 2020: Crypto Valley Blockchain Conference.

Program Committee

- 2025: Usenix Security
- 2024: FC, CCS (**Top reviewer award**), AFT
- 2023: Usenix Security (**Noteworthy reviewer award**), NDSS, CSF, FC, CCS (**Best reviewer award**)
- 2022: S&P, NDSS, FC, EuroS&P, CAAW (WWW workshop), AFT, CESC, DeFi (CCS Workshop)
- 2021: FC **(selected as A+ reviewer)**, NDSS, CCS, CVC, TPBC, CBT, DeFi (CCS Workshop)
- 2020: Cryptoeconomic Systems, IEEE DAPPS, Marble, IEEE S&B, WPES, CBT
- 2019: ICBC, CNS, IEEE S&B, CBT, Marble, Blockchain
- 2018: CBT, WPES, Blockchain, BlockSEA, SOCCA

Editorial Board & Journal Reviewer

- 2025: PETS
- 2024: PETS, Transactions on Dependable and Secure Computing
- 2023: PETS
- 2022: Journal Blockchain Research and Applications., Journal of Parallel and Distributed Computing

- 2021: PETS
- 2020: PETS, Journal of Cryptoeconmic Systems, Security & Privacy, Transactions on Networking
- 2019: PETS **(Best reviewer award)**, Journal of Cooperative Information Systems, Transactions on Internet Technology, Journal of Cooperative Information Systems, Transactions on Dependable and Secure Computing, Frontiers Blockchain (Non-Financial Blockchain), IEEE Computers, IET Information Security
- 2018: PETS, Journal of Computer Security, Transactions on Dependable and Secure Computing, Transactions on Computers, Frontiers Blockchain (Non-Financial Blockchain)

PhD Thesis Committee

- 2024: Dimitris Kolonelos, Universidad Politecnica de Madrid (UPM)
- 2023: Connor Macmenamin, Universtiy Pompeu Fabra (UPF)
- 2022: George Kappos, University College Londong (UCL)

Research/Travel Grants

- 2022: PC member for the NDSS travel grants, Remote Referee for ERC
- 2021: Panel for the Israel Science Foundation

Organization Committee

- 2019: 1st International Summer School on Security & Privacy for Blockchains and Distributed Ledger Technologies.

RESEARCH IMPLEMENTED IN INDUSTRY

1. Implementation of the Generalized Bitcoin-Compatible Channels
   `https://github.com/comit-network/thor`
2. Introduce first version of ECDSA adaptor signature spec
   `https://github.com/discreetlogcontracts/dlcspecs/pull/114`
3. A2L Proof of Concept on top of Bitcoin
   `https://github.com/comit-network/a2l-poc`
4. CoinShuffle++ implementation for Decred
   `https://blog.decred.org/2019/08/28/Iterating-Privacy/`
5. 2P-ECDSA Signatures for the Lightning Network
   `https://github.com/cfromknecht/tpec`
6. ECDSA based construction for Anonymous Multi-Hop Locks
   `https://github.com/KZen-networks/multi-hop-locks`
7. An implementation of the CoinShuffle protocol in Java for MyCellium wallet
   `https://github.com/nekosune/shuffle-java`
8. CoinShuffle implementation for NXT cryptocurrency
   `https://github.com/mrv777/NXT`
9. Implementation of the CashShuffle protocol for privacy-enhanced transactions on Bitcoin Cash, based on CoinShuffle
   `https://npm.pkg.github.com/MaxXor/CashShuffle`

10. Nagzul library including an implementation of DLSAG: Non-Interactive Refund Transactions For Interoperable Payment Channels in Monero
`https://github.com/edwinhere/nazgul`