Alessandro Chiesa

Curriculum Vitae
(last updated: 2025)

Personal Information

Email: alessandro.chiesa@epfl.ch
Homepage: https://ic-people.epfl.ch/~achiesa/
Birth place & date: Varese (Italy) on October 3, 1987
Nationality: Italian citizen & Swiss permanent resident
Languages: Italian (fluent), English (fluent), Russian (conversational), German (conversational)

Research Interests

Cryptography, Security, Complexity Theory

Academic Appointments

EPFL, **Tenured Associate Professor**, Computer and Communication Sciences, 09.2021 – present

UC Berkeley, **Tenured Associate Professor**, EECS, 07.2021 – 06.2023

UC Berkeley, **Assistant Professor**, EECS, 07.2015 – 07.2021

ETH Zürich, **Postdoctoral Researcher**, Computer Science, 09.2014 – 07.2015

Education

MIT, **Ph.D.**, Electrical Engineering and Computer Science, September 2014
- Thesis: *Succinct Non-Interactive Arguments*
- Advisor: Prof. Silvio Micali

MIT, **M.Eng.**, Electrical Engineering and Computer Science, June 2010
- Thesis: *Proof-Carrying Data*
- Advisors: Prof. Ronald L. Rivest and Prof. Eran Tromer

MIT, **S.B.**, Mathematics, June 2009

MIT, **S.B.**, Computer Science and Engineering, June 2009

Awards

- Best Paper Award at CRYPTO 2024 (recognizes the paper "STIR: Reed–Solomon Proximity Testing with Fewer Queries" for a breakthrough result)
- Test of Time Award at IEEE SP 2024 (recognizes the paper "Zerocash: Decentralized Anonymous Payments from Bitcoin" for broad and lasting impact on both research and practice in computer security and privacy)
- MIT Technology Review's "35 Innovators Under 35" in 2018 (names the world's top 35 innovators under the age of 35)
- Charles and Jennifer Johnson Thesis Award in 2010 (for best computer science M.Eng. theses at MIT)

Companies Founded

StarkWare Industries (`https://www.starkware.co/`), 2017

- Pioneered and deployed scalability solutions for peer-to-peer smart contract systems such as Ethereum, based on succinct arguments. This company has helped secure almost a billion transactions amounting to over a trillion dollars in exchanged value, and is a market leader for "layer 2 rollups" on Ethereum.

The Zcash Company (`https://z.cash/`), 2014

- Launched Zcash, a cryptocurrency that provides strong user privacy guarantees (based on a protocol I co-invented). This company pioneered the first large-scale deployment of zero knowledge succinct arguments.

Open-Source Libraries

`arkworks` (`https://github.com/arkworks-rs`) (2017 – present)

- Oversaw the development of well-known open-source libraries for succinct cryptographic proofs. These have 3500+ stars on GitHub, have been widely used by research groups, by open-source, and by companies.

Advising

Postdoctoral Researchers

- Igor Shinkar (August 2016 – June 2018)
  now Assistant Professor at Simon Fraser University
- Tom Gur (April 2017 – December 2018)
  now Professor at the University of Cambridge
- Jonathan Bootle (August 2019 – August 2020)
  now Researcher at IBM Zurich
- Katerina Sotiraki (August 2020 – August 2022)
  now Assistant Professor at Yale University
- Michele Orrù (August 2020 – August 2022)
  now Assistant Professor at CNRS in Sorbonne Université
- Sarah Bordage (July 2022 – September 2023)
- Ngoc Khanh Nguyen (September 2022 – October 2023)
  now Assistant Professor at King's College London

PhD Students

- Nicholas Spooner (thesis completed in June 2020)
  Thesis: *Succinct Non-Interactive Arguments for Arithmetic Circuits*
  now Assistant Professor at Cornell University
- Lynn Chua (thesis completed in June 2020, co-advised with Bernd Sturmfels)
  Thesis: *Discrete and Complex Algorithms for Curves*
- Pratyush Mishra (thesis completed in September 2021, co-advised with Raluca A. Popa)
  Thesis: *Privacy and Scalability for Decentralized Cryptographic Systems*
  now Assistant Professor at the University of Pennsylvania
- Yuncong Hu (thesis completed in May 2022, co-advised with Raluca A. Popa)
  Thesis: *Decentralized Ledgers: Design and Applications*
  now Assistant Professor at Shanghai Jiao Tong University
- Siqi Liu (thesis completed in August 2023)
  Thesis: *Geometry of Local-Spectral Expanders*
  now Postdoctoral Researcher at the Institute of Advanced Study, Princeton
- Ziyi Guan (thesis in progress)
  Research topics: Complexity Theory and Cryptography
- Giacomo Fenzi (thesis in progress)
  Research topics: Complexity Theory and Cryptography
- Zijing Di (thesis in progress)
  Research topics: Post-Quantum and Quantum Cryptography
- Yuxi Zheng (thesis in progress)
  Research topics: Complexity Theory and Cryptography
- Christian Knabenhans (thesis in progress)
  Research topics: Lattice and Applied Cryptography
- Guy Weissenberg (thesis in progress)
  Research topics: Probabilistic Proofs
- Burcu Yıldız (thesis in progress)
  Research topics: Probabilistic Proofs
- Zihan Hu (thesis in progress)
  Research topics: Quantum Cryptography

MS Students

- Nicholas Spooner (thesis completed in April 2015, co-advised with Thomas Holenstein)
  Thesis: *Interactive Oracle Proofs*
- Jiahao Wang (thesis completed in August 2016)
  Thesis: *Scaling out Proof Systems on Spark*
- Howard Wu (thesis completed in May 2018)
  Thesis: *DIZK: A Distributed Zero Knowledge Proof System*

- Nicholas Ward (thesis completed in May 2021)
  Thesis: *Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS*
- Mathias Marty (thesis completed in June 2024)
  Thesis: *On State-Restoration Knowledge Soundness from Special Soundness*
- Hossein Moghaddas (thesis completed in July 2024)
  Thesis: *On Proximity Testing of Reed–Solomon Codes and Polynomial Interactive Oracle Proofs*
- Jérémi Do Dinh (thesis completed in September 2024)
  Thesis: *Simulation Security in the Random Oracle Model*
- Burcu Yıldız (thesis completed in December 2024)
  Thesis: *On Parallel Repetition of PCPs*

Workshops

I led the organization of the following workshops and programs.

- *Foundations and Frontiers of Probabilistic Proofs* (2-week **MSRI summer school** in July 2023)
- *Efficient Probabilistic Proofs* (1-week **Bertinoro workshop** in July 2022)
- *Foundations and Frontiers of Probabilistic Proofs* (2-week **MSRI summer school** in July 2021)
- *Proofs, Consensus, and Decentralizing Society* (Fall 2019, **semester program @ Simons Institute**)
- *Decentralized Cryptocurrencies and Blockchains* (workshop at CRYPTO 2018)
- *Probabilistically Checkable and Interactive Proofs* (workshop at STOC 2017 Theory Fest)
- *8th Conference on Innovations in Theoretical Computer Science* (ITCS 2017)

Teaching

- Sp2025, *CS250: Algorithms I* (undergraduate)
- Fa2024, *CS459: Foundations of Probabilistic Proofs* (graduate)
- Sp2024, *CS523: Advanced Topics on Privacy Enhancing Technologies* (graduate)
- Fa2023, *CS459: Foundations of Probabilistic Proofs* (graduate)
- Sp2023, *CS450: Advanced Algorithms* (undergraduate)
- Fa2022, *CS459: Foundations of Probabilistic Proofs* (graduate)
- Sp2022, *CS602: Foundations of Probabilistic Proofs* (graduate)
- Fa2021, *Teaching Leave*
- Sp2021, *CS170: Efficient Algorithms and Intractable Problems* (undergraduate, 612 students)
- Fa2020, *CS294: Foundations of Probabilistic Proofs* (graduate)
- Sp2020, *CS170: Efficient Algorithms and Intractable Problems* (undergraduate, 658 students)
- Fa2019, *Teaching Leave (running a semester program at the Simons Institute)*
- Sp2019, *CS294: Probabilistically Checkable and Interactive Proof Systems* (graduate)
- Fa2018, *CS170: Efficient Algorithms and Intractable Problems* (undergraduate, 878 students)
- Sp2018, *CS170: Efficient Algorithms and Intractable Problems* (undergraduate, 608 students)
- Fa2017, *CS276: Cryptography* (graduate)
- Sp2017, *CS294: Probabilistically Checkable and Interactive Proof Systems* (graduate)

- Fa2016, *CS294: Property Testing* (graduate)
- Sp2016, *CS170: Efficient Algorithms and Intractable Problems* (undergraduate, 460 students)
- Fa2015, *CS276: Cryptography* (graduate)

Publications [click here for Google Scholar profile]

Books

[1] *Building Cryptographic Proofs from Hash Functions*
Alessandro Chiesa, Eylon Yogev
https://snargsbook.org/

Journal publications

[2] *Succinct Non-Interactive Arguments via Linear Interactive Proofs* (journal version of [66])
Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, Omer Paneth
Journal of Cryptology (Volume 35, Issue 3, May 2022)

[3] *Spatial Isolation Implies Zero Knowledge Even in a Quantum World* (journal version of [45])
Alessandro Chiesa, Michael A. Forbes, Tom Gur, Nicholas Spooner
Journal of the ACM (Volume 69, Issue 2, April 2022, Article Number 15)

[4] *On Axis-Parallel Tests for Tensor Product Codes* (journal version of [51])
Alessandro Chiesa, Peter Manohar, Igor Shinkar
Theory of Computing Journal (Volume 6, Article 5, 2020)

[5] *Testing Linearity against Non-Signaling Strategies* (journal version of [47])
Alessandro Chiesa, Peter Manohar, Igor Shinkar
ACM Transactions on Computation Theory (Volume 12, Issue 3, 2020)

[6] *On Cycles of Pairing-Friendly Elliptic Curves*
Alessandro Chiesa, Lynn Chua, Matthew Weidner
SIAM Journal on Applied Algebra and Geometry (Volume 3, Issue 2, 2019)

[7] *Scalable Zero Knowledge via Cycles of Elliptic Curves* (journal version of [59])
Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza
Algorithmica (Volume 79, Issue 4, 2017)

[8] *The Hunting of the SNARK* (journal version of [69])
Nir Bitansky, Ran Canetti, Alessandro Chiesa, Shafi Goldwasser, Huijia Lin, Aviad Rubinstein, Eran Tromer
Journal of Cryptology (Volume 30, Issue 4, 2017)

[9] *Knightian Analysis of the Vickrey Mechanism*
Alessandro Chiesa, Silvio Micali, Zeyuan Allen Zhu
Econometrica (Volume 83, Issue 5, 2015)

[10] *Improved Soundness for QMA with Multiple Provers*
Alessandro Chiesa, Michael A. Forbes

Chicago Journal of Theoretical Computer Science (2013)

[11] *Proof-carrying data: Secure computation on untrusted platforms*
Alessandro Chiesa, Eran Tromer
The Next Wave: The NSA's review of emerging technologies (Vol.19, No.2, 2012)

Refereed conferences

[12] *zkSNARKs in the ROM with Unconditional UC-Security*
Alessandro Chiesa, Giacomo Fenzi
TCC 2024 (22nd Theory of Cryptography Conference)

[13] *Untangling the Security of Kilian's Protocol: Upper and Lower Bounds*
Alessandro Chiesa, Marcel Dall'Agnol, Ziyi Guan, Nicholas Spooner, Eylon Yogev
TCC 2024 (22nd Theory of Cryptography Conference)

[14] *Security Bounds for Proof-Carrying Data from Straightline Extractors*
Alessandro Chiesa, Ziyi Guan, Shahar Samocha, Eylon Yogev
TCC 2024 (22nd Theory of Cryptography Conference)

[15] *STIR: Reed–Solomon Proximity Testing with Fewer Queries*
Gal Arnon, Alessandro Chiesa, Giacomo Fenzi, Eylon Yogev
CRYPTO 2024 (44th International Cryptology Conference)
Best Paper Award (awarded to two papers in this conference)

[16] *On Parallel Repetition of PCPs*
Alessandro Chiesa, Ziyi Guan, Burcu Yıldız
ITCS 2024 (15th Conference on Innovations in Theoretical Computer Science)

[17] *IOPs with Inverse Polynomial Soundness Error*
Gal Arnon, Alessandro Chiesa, Eylon Yogev
FOCS 2023 (64th IEEE Symposium on Foundations of Computer Science)

[18] *Lattice-Based Succinct Arguments for NP with Polylogarithmic-Time Verification*
Jonathan Bootle, Alessandro Chiesa, Katerina Sotiraki
CRYPTO 2023 (43rd International Cryptology Conference)

[19] *EOS: Efficient Private Delegation of zkSNARK Provers*
Alessandro Chiesa, Ryan Lehmkuhl, Pratyush Mishra, Yinuo Zhang
USENIX Security 2023 (32nd USENIX Security Symposium)

[20] *Proof-Carrying Data From Arithmetized Random Oracles*
Megan Chen, Alessandro Chiesa, Tom Gur, Jack O'Connor, Nicholas Spooner
EUROCRYPT 2023 (42nd Conference on the Theory and Applications of Cryptographic Techniques)

[21] *A Toolbox for Barriers on Interactive Oracle Proofs*
Gal Arnon, Amey Bhangale, Alessandro Chiesa, Eylon Yogev
TCC 2022 (20th Theory of Cryptography Conference)

[22] *Hardness of Approximation for Stochastic Problems via Interactive Oracle Proofs*
Gal Arnon, Alessandro Chiesa, Eylon Yogev
CCC 2022 (37th Computational Complexity Conference)

[23] *On Succinct Non-Interactive Arguments in Relativized Worlds*
Megan Chen, Alessandro Chiesa, Nicholas Spooner
EUROCRYPT 2022 (41st Conference on the Theory and Applications of Cryptographic Techniques)

[24] *Gemini: Elastic SNARKs for Diverse Environments*
Jonathan Bootle, Alessandro Chiesa, Yuncong Hu, Michele Orrù
EUROCRYPT 2022 (41st Conference on the Theory and Applications of Cryptographic Techniques)

[25] *A PCP Theorem for Interactive Proofs and Applications*
Gal Arnon, Alessandro Chiesa, Eylon Yogev
EUROCRYPT 2022 (41st Conference on the Theory and Applications of Cryptographic Techniques)

[26] *Zero-Knowledge IOPs with Linear-Time Prover and Polylogarithmic-Time Verifier*
Jonathan Bootle, Alessandro Chiesa, Siqi Liu
EUROCRYPT 2022 (41st Conference on the Theory and Applications of Cryptographic Techniques)

[27] *Tight Security Bounds for Micali's SNARGs*
Alessandro Chiesa, Eylon Yogev
TCC 2021 (19th Theory of Cryptography Conference)

[28] *Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier*
Alessandro Chiesa, Fermi Ma, Nicholas Spooner, Mark Zhandry
FOCS 2021 (62nd IEEE Symposium on Foundations of Computer Science) (**invited to SICOMP special issue**)
QCrypt 2021 (11th edition of the yearly conference presenting last year's top results in quantum cryptography)
QIP 2022 (25th Conference on Quantum Information Processing)

[29] *Sumcheck Arguments and their Applications*
Jonathan Bootle, Alessandro Chiesa, Katerina Sotiraki
CRYPTO 2021 (41st International Cryptology Conference)

[30] *Subquadratic SNARGs in the Random Oracle Model*
Alessandro Chiesa, Eylon Yogev
CRYPTO 2021 (41st International Cryptology Conference)

[31] *Proof-Carrying Data without Succinct Arguments*
Bendikt Bünz, Alessandro Chiesa, William Lin, Pratyush Mishra, Nicholas Spooner
CRYPTO 2021 (41st International Cryptology Conference)

[32] *Proof-Carrying Data from Accumulation Schemes*
Bendikt Bünz, Alessandro Chiesa, Pratyush Mishra, Nicholas Spooner
TCC 2020 (18th Theory of Cryptography Conference)

[33] *Barriers for Succinct Arguments in the Random Oracle Model*
Alessandro Chiesa, Eylon Yogev
TCC 2020 (18th Theory of Cryptography Conference)

[34] *Linear-Time Arguments with Sublinear Verification from Tensor Codes*
Jonathan Bootle, Alessandro Chiesa, Jens Groth
TCC 2020 (18th Theory of Cryptography Conference)

[35] *Fractal: Post-Quantum and Transparent Recursive Proofs from Holography*
Alessandro Chiesa, Dev Ojha, Nicholas Spooner
EUROCRYPT 2020 (39th Conference on the Theory and Applications of Cryptographic Techniques)

[36] *Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS*
Alessandro Chiesa, Yuncong Hu, Mary Maller, Pratyush Mishra, Noah Vesely, Nicholas P. Ward
EUROCRYPT 2020 (39th Conference on the Theory and Applications of Cryptographic Techniques)

[37] *On the Impossibility of Probabilistic Proofs in Relativized Worlds*
Alessandro Chiesa, Siqi Liu
ITCS 2020 (11th Conference on Innovations in Theoretical Computer Science)

[38] *On Local Testability in the Non-Signaling Setting*
Alessandro Chiesa, Peter Manohar, Igor Shinkar
ITCS 2020 (11th Conference on Innovations in Theoretical Computer Science)

[39] *ZEXE: Enabling Decentralized Private Computation*
Sean Bowe, Alessandro Chiesa, Matthew D. Green, Ian Miers, Pratyush Mishra, Howard Wu
S&P 2020 (41st IEEE Symposium on Security and Privacy)

[40] *Relaxed Locally Correctable Codes with Nearly-Linear Block Length and Constant Query Complexity*
Alessandro Chiesa, Tom Gur, Igor Shinkar
SODA 2020 (31st Symposium on Discrete Algorithms)

[41] *Succinct Arguments in the Quantum Random Oracle Model*
Alessandro Chiesa, Peter Manohar, Nicholas Spooner
TCC 2019 (17th Theory of Cryptography Conference)
QIP 2020 (23rd Conference on Quantum Information Processing)

[42] *Linear-Size Constant-Query IOPs for Delegating Computation*
Eli Ben-Sasson, Alessandro Chiesa, Lior Goldberg, Tom Gur, Michael Riabzev, Nicholas Spooner
TCC 2019 (17th Theory of Cryptography Conference)

[43] *Aurora: Transparent Succinct Arguments for R1CS*
Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, Nicholas P. Ward
EUROCRYPT 2019 (38th Conference on the Theory and Applications of Cryptographic Techniques)

[44] *Probabilistic Checking against Non-Signaling Strategies from Linearity Testing*
Alessandro Chiesa, Peter Manohar, Igor Shinkar
ITCS 2019 (10th Conference on Innovations in Theoretical Computer Science)

[45] *Spatial Isolation Implies Zero Knowledge Even in a Quantum World*
Alessandro Chiesa, Michael A. Forbes, Tom Gur, Nicholas Spooner
FOCS 2018 (59th IEEE Symposium on Foundations of Computer Science)
QIP 2019 (22nd Conference on Quantum Information Processing)

[46] *DIZK: A Distributed Zero Knowledge Proof System*
Howard Wu, Wenting Zheng, Alessandro Chiesa, Raluca A. Popa, Ion Stoica
USENIX Security 2018 (27th USENIX Security Symposium)

[47] *Testing Linearity against Non-Signaling Strategies*
Alessandro Chiesa, Peter Manohar, Igor Shinkar
CCC 2018 (33rd Computational Complexity Conference)

[48] *Oblix: An Efficient Oblivious Search Index*
Pratyush Mishra, Rishabh Poddar, Jerry Chen, Alessandro Chiesa, Raluca A. Popa
S&P 2018 (39th IEEE Symposium on Security and Privacy)

[49] *Proofs of Proximity for Distribution Testing*
Alessandro Chiesa, Tom Gur
ITCS 2018 (9th Conference on Innovations in Theoretical Computer Science)

[50] *Zero Knowledge Protocols from Succinct Constraint Detection*
Eli Ben-Sasson, Alessandro Chiesa, Michael A. Forbes, Ariel Gabizon, Michael Riabzev, Nicholas Spooner
TCC 2017 (15th Theory of Cryptography Conference)

[51] *On Axis-Parallel Tests for Tensor Product Codes*
Alessandro Chiesa, Peter Manohar, Igor Shinkar
RANDOM 2017 (21st International Workshop on Randomization and Computation)

[52] *Interactive Oracle Proofs with Constant Rate and Query Complexity*
Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, Michael Riabzev, Nicholas Spooner
ICALP 2017 (44th International Colloquium on Automata, Languages, and Programming)

[53] *Decentralized Anonymous Micropayments*
Alessandro Chiesa, Matthew D. Green, Jingcheng Liu, Peihan Miao, Ian Miers, Pratyush Mishra
EUROCRYPT 2017 (36th Conference on the Theory and Applications of Cryptographic Techniques)

[54] *Computational Integrity with a Public Random String from Quasilinear PCPs*
Eli Ben-Sasson, Iddo Bentov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, Madars Virza
EUROCRYPT 2017 (36th Conference on the Theory and Applications of Cryptographic Techniques)

[55] *Interactive Oracle Proofs*
Eli Ben-Sasson, Alessandro Chiesa, Nicholas Spooner
TCC 2016-B (14th Theory of Cryptography Conference)

[56] *Quasilinear-Size Zero Knowledge from Linear-Algebraic PCPs*
Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, Madars Virza
TCC 2016-A (13th Theory of Cryptography Conference)

[57] *Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs*
Eli Ben-Sasson, Alessandro Chiesa, Matthew D. Green, Eran Tromer, Madars Virza
S&P 2015 (36th IEEE Symposium on Security and Privacy)

[58] *Cluster Computing in Zero Knowledge*
Alessandro Chiesa, Eran Tromer, Madars Virza
EUROCRYPT 2015 (34th Conference on the Theory and Applications of Cryptographic Techniques)

[59] *Scalable Zero Knowledge via Cycles of Elliptic Curves*
Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza
CRYPTO 2014 (34th International Cryptology Conference)

[60] *Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture*
Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza
USENIX Security 2014 (23rd USENIX Security Symposium)

[61] *Knightian Self Uncertainty in the VCG Mechanism for Unrestricted Combinatorial Auctions*
Alessandro Chiesa, Silvio Micali, Zeyuan Allen Zhu
EC 2014 (15th ACM Conference on Economics and Computation)

[62] *Zerocash: Decentralized Anonymous Payments from Bitcoin*
Eli Ben-Sasson, Alessandro Chiesa, Christina L. Garman, Matthew D. Green, Ian Miers, Eran Tromer, Madars Virza
S&P 2014 (35th IEEE Symposium on Security and Privacy)
IEEE SP Test-of-Time Award in 2024 (substantial impact on the field of security and privacy)

[63] *SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge*
Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, Madars Virza
CRYPTO 2013 (33rd International Cryptology Conference)

[64] *On the Concrete Efficiency of Probabilistically-Checkable Proofs*
Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer
STOC 2013 (45th ACM Symposium on the Theory of Computing)

[65] *Recursive Composition and Bootstrapping for SNARKs and Proof-Carrying Data*
Nir Bitansky, Ran Canetti, Alessandro Chiesa, Eran Tromer
STOC 2013 (45th ACM Symposium on the Theory of Computing)

[66] *Succinct Non-Interactive Arguments via Linear Interactive Proofs*
Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, Omer Paneth
TCC 2013 (10th Theory of Cryptography Conference)

[67] *Fast Reductions from RAMs to Delegatable Succinct Constraint Satisfaction Problems*
Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer
ITCS 2013 (4th Conference on Innovations in Theoretical Computer Science)

[68] *Succinct Arguments from Multi-Prover Interactive Proofs and their Efficiency Benefits*
Nir Bitansky, Alessandro Chiesa
CRYPTO 2012 (32nd International Cryptology Conference)

[69] *From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again*
Nir Bitansky, Ran Canetti, Alessandro Chiesa, Eran Tromer
ITCS 2012 (3rd Conference on Innovations in Theoretical Computer Science)

[70] *Mechanism Design with Approximate Valuations*
Alessandro Chiesa, Silvio Micali, Zeyuan Allen Zhu
ITCS 2012 (3rd Conference on Innovations in Theoretical Computer Science)

[71] *Proof-Carrying Data and Hearsay Arguments from Signature Cards*
Alessandro Chiesa, Eran Tromer
ITCS 2010 (1st Conference on Innovations in Theoretical Computer Science)

Theses

[72] *Succinct Non-Interactive Arguments*
Ph.D. thesis at MIT (September 2014)
Advised by Prof. Silvio Micali

[73] *Proof-Carrying Data*
M.Eng. thesis at MIT (June 2010)
Advised by Prof. Ronald L. Rivest and Prof. Eran Tromer

Lectures

STIR: Reed–Solomon Proximity Testing with Fewer Queries

[L95] 2024-08-06, StarkWare Scholar Summit (Cornell Tech, New York, NY)

Building Succinct Arguments From Ideal Hash Functions

[L94] 2024-06-27, Cryptography Seminar (Bocconi University, Milano, Italy)

[L93] 2024-05-31, MIT CIS Seminar (MIT, Cambridge, MA)

[L92] 2024-05-22, ZKProof 6 (Berlin, Germany)

Subquadratic SNARGs in the Random Oracle Model

[L91] 2023-11-08, Stanford Security Seminar (Palo Alto, CA)

[L90] 2023-09-08, Swiss Crypto Day (ETH Zurich)

Privacy Applications of zkSNARKs to Blockchains

[L89] 2023-04-12, Guest lecture at DeCenter (Princeton University (online))

Security Bounds for Succinct Arguments from Hash Functions

[L88] 2023-02-06, StarkWare Sessions (Tel-Aviv, Israel)

How to Verify Computations without Re-Executing Them?

[L87] 2022-11-15, Inaugural Lecture at EPFL (Lausanne, Switzerland)

Privacy and Scalability Applications of zkSNARKs to Blockchains

[L86] 2022-06-03, SNB-CIF Conference on Cryptoassets and Financial Innovation (Zurich, Switzerland)

[L85] 2022-01-20, Swiss National Bank Technology & Finance Seminar (Virtual Event)

Digital Assets: Privacy and Scalability Challenges

[L84] 2021-11-05, Finance and Technology Conference (Lausanne, Switzerland)

How to Make SNARKs

[L83] 2021-10-26, ZK Hack (Virtual Event)

From Zero Knowledge to Private Transactions

[L82] 2021-02-24, Distinguished Lecture (Sapienza University of Rome)

An Introduction to Recursive SNARKs

[L81] 2020-08-21, International Joint Conference on Theoretical Computer Science (Virtual)

[L80] 2020-07-09, Crypto Economics Security Conference (San Francisco, CA)

A Framework for Efficient STARKs

[L79] 2020-01-06, ZK Global (Tel Aviv, Israel)

[L78] 2019-11-25, ZKP Meetup (San Francisco, CA)

Marlin: Preprocessing zkSNARKs with Universal Setup

[L77] 2019-10-28, Crypto Economics Security Conference (San Francisco, CA)

State of the SNARG-scape

[L76] 2019-12-16, Web3 Foundation (Zug, Switzerland)

[L75] 2019-10-26, Zero Knowledge Summit (San Francisco, CA)

From Holography to Recursive Proofs

[L74] 2019-09-24, Workshop on Probabilistically Checkable and Interactive Proof Systems (Berkeley, CA)

Succinct Arguments

[L73] 2019-08-27, Bootcamp for "Proofs, Consensus, and Decentralizing Society" (Berkeley, CA)

A Framework for Post-Quantum Succinct Arguments

[L72] 2019-06-23, Zcon1 (Split, Croatia)

[L71] 2019-04-12, ZKP Standards Workshop (Berkeley, CA)

From Zero Knowledge to Private Transactions

[L70] 2019-09-19, Seminar at the Simons Institute (Berkeley, CA)

[L69] 2019-04-13, ZK Day at the Simons Institute (Berkeley, CA)

Aurora: Transparent Succinct Arguments for R1CS

[L68] 2019-01-30, Stanford Blockchain Conference (Palo Alto, CA)

ZEXE: Enabling Decentralized Private Computation

[L67] 2019-06-03, Sony Corporation R&D Center (Tokyo, Japan)

[L66] 2018-12-19, DFINITY (Zurich, Switzerland)

Zero Knowledge Succinct Arguments

[L65] 2018-12-05, Bitcoin Meetup Switzerland (Zurich, Switzerland)

Transparent Succinct Arguments

[L64] 2018-10-15, Scalar Capital Summit (San Francisco, CA)

[L63] 2018-10-10, Crypto Economics Security Conference (San Francisco, CA)

[L62] 2018-09-22, Blockchain Research Center Workshop (Stanford University, CA)

Succinct Arguments from Interactive Oracle Proofs

[L61] 2018-06-20, Crypto Valley Conference (Zug, Switzerland)

[L60] 2018-06-17, Cryptography Seminar (Tel Aviv University, Israel)

Zerocash: addressing Bitcoin's privacy problem

[L59] 2017-10-02, Crypto Economics Security Conference (Berkeley, CA)

[L58] 2017-08-28, Google Tech Talk (Mountain View, CA)

[L57] 2017-06-08, Summer School on Real World Crypto and Privacy (Šibenik, Croatia)

[L56] 2015-06-01, IBM Research (Zurich, Switzerland)

Bitcoin, Its Privacy Problem, and How to Fix It

[L55] 2018-10-08, CS KickStart (Berkeley, CA)

[L54] 2018-23-07, Blockchain Technology and Theory @ PODC 2018 (Royal Holloway, University of London, UK)

[L53] 2018-18-06, Cyber Week (Tel Aviv, Israel)

[L52] 2017-12-05, Credit Suisse ITS Academy (Zurich, Switzerland)

[L51] 2017-09-25, Math Lovers Forum (Woodside, CA)

Succinct Arguments: Constructions and Open Problems

[L50] 2017-06-23, Workshop at STOC 2017 Theory Fest (Montreal, Canada)

From Algebraic Complexity to Zero Knowledge Protocols

[L49] 2017-03-24, MIT CIS Seminar (MIT, Cambridge, MA)

[L48] 2017-03-07, Security Seminar (Stanford University, CA)

Zero Knowledge Succinct Arguments: an Introduction

[L47] 2017-06-06, Summer School on Real World Crypto and Privacy (Šibenik, Croatia)

[L46] 2017-03-24, Guest lecture in "6.892: Shared Public Ledgers" (MIT, Cambridge, MA)

[L45] 2017-02-24, Coinbase (San Francisco, CA)

Decentralized Anonymous Micropayments

[L44] 2017-03-23, Security Seminar (Boston University, Boston, MA)

[L43] 2016-12-07, Security Seminar (ETH Zurich, Switzerland)

[L42] 2016-11-10, Visa Research (Foster City, CA)

State of the SNARK

[L41] 2016-10-22, Ethereum Silicon Valley Meetup (Foster City, CA)

Probabilistic checking and interaction

[L40] 2016-08-10, Simons Institute Cryptography Reunion (Berkeley, CA)

[L39] 2016-07-13, DIMACS Workshop on Cryptography and its Interactions (Rutgers University, New Brunswick, NJ)

Cycles of elliptic curves: applications and open problems

[L38] 2016-05-04, Number Theory Seminar (UC Berkeley, Berkeley, CA)

[L37] 2015-12-16, Seminar on Coding Theory and Cryptography (University of Zurich, Zurich, Switzerland)

Interactive oracle proofs

[L36] 2015-10-14, Theory Lunch (Berkeley, CA)

Cluster Computing in Zero Knowledge

[L35] 2015-04-28, EUROCRYPT 2015 (Sofia, Bulgaria)

libsnark: a C++ library for SNARK proofs

[L34] 2015-04-26, COST CryptoAction Meeting @ Eurocrypt 2015 (Sofia, Bulgaria)

Scalable Zero Knowledge via Cycles of Elliptic Curves

[L33] 2014-11-13, Greater Tel Aviv Area Crypto Symposium (Tel Aviv University, Israel)

[L32] 2014-10-24, Charles River Crypto Day (MIT, Cambridge, MA)

[L31] 2014-10-01, Cryptography Seminar (ETH Zurich, Switzerland)

[L30] 2014-08-21, CRYPTO 2014 (Santa Barbara, CA)

[L29] 2014-08-14, Crypto Seminar (UCSD, La Jolla, CA)

[L28] 2014-08-08, Crypto Research Group Seminar (IBM Watson Research Center, Yorktown, NY)

[L27] 2014-07-23, Cryptography Seminar (Bar Ilan University, Israel)

[L26] 2014-07-21, Computer Science Colloquium (Technion, Israel)

Succinct Non-Interactive Zero Knowledge

[L25] 2014-03-31, Theory Seminar (Berkeley University, CA)

[L24] 2014-03-25, Security Seminar (1)

[L23] 2014-03-14, Theory Lunch (Princeton University, Princeton, NJ)

SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge

[L22] 2013-11-22, MIT CIS Seminar (MIT, Cambridge, MA)

[L21] 2013-11-15, CryptoDay at NYU (New York University, NY)

On the Concrete Efficiency of Probabilistically-Checkable Proofs

[L20] 2013-07-16, Complexity Seminar (Tel Aviv University, Israel)

[L19] 2013-06-03, STOC 2013 (Palo Alto, CA)

Recursive Composition and Bootstrapping for SNARKs and Proof-Carrying Data

[L18] 2013-06-02, STOC 2013 (Palo Alto, CA)

Succinct Non-Interactive Arguments from Linear Interactive Proofs

[L17] 2013-07-11, Cryptography Seminar (Tel Aviv University, Israel)

[L16] 2013-05-16, MIT CIS Seminar (MIT, Cambridge, MA)

[L15] 2013-03-05, TCC 2013 (Tokyo University, Tokyo, Japan)

A New Construction of Publicly-Verifiable Non-Interactive Succinct Arguments

[L14] 2013-01-15, Security Seminar (Stanford University, CA)

Succinct Arguments from Multi-Prover Interactive Proofs and their Efficiency Benefits

[L13] 2012-08-21, CRYPTO 2012 (Santa Barbara, CA)

How Multi-Prover Interactive Proofs and Proof-Carrying Data Make Delegation More Affordable

[L12] 2012-10-15, Security Seminar (Boston University, Boston, MA)

[L11] 2012-08-02, Cryptography Seminar (Tel Aviv University, Israel)

[L10] 2012-06-29, CryptoDay on Delegating Computation (Columbia University, NY)

Fast Reductions from RAMs to Delegatable Succinct Constraint Satisfaction Problems

[L9] 2013-01-12, ITCS 2013 (Berkeley University, CA)

[L8] 2012-08-09, Cryptography Seminar (Tel Aviv University, Israel)

[L7] 2012-06-28, Crypto Research Group Seminar (IBM Watson Research Center, Hawthorne, NY)

[L6] 2012-05-27, MIT CIS Seminar (MIT, Cambridge, MA)

From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again

[L5] 2012-01-10, ITCS 2012 (Cambridge, MA)

Mechanism Design with Approximate Valuations

[L4] 2012-07-26, 4th World Congress of the Game Theory Society (Bilgi University, Istanbul, Turkey)

[L3] 2012-01-08, ITCS 2012 (Cambridge, MA)

[L2] 2011-06-15, CS Algorithms Seminar (Tel Aviv University, Israel)

Proof-Carrying Data

[L1] 2010-01-06, ITCS 2010 (Tsinghua University, Beijing, China)