# Nicholas Spooner

✉ *nspooner@cornell.edu*
🔗 *spooner.cc*

## Academic positions

2024–present **Assistant Professor**, *Cornell University*, USA.

2023–2024 **Visiting Assistant Professor**, *New York University*, USA.

2022–2024 **Assistant Professor**, *University of Warwick*, UK.

2020–2021 **Postdoctoral Associate**, *Boston University*, USA.

## Education

2017–2020 **PhD**, *University of California, Berkeley*, USA.
Thesis: *Succinct Non-Interactive Arguments for Arithmetic Circuits.*
Advisor: Alessandro Chiesa.

2015–2017 **PhD (transferred out)**, *University of Toronto*, Canada.
Advisor: Toniann Pitassi.

2013–2015 **MSc Computer Science**, *ETH Zürich*, Switzerland.
Thesis: *Interactive oracle proofs.* Advisors: Thomas Holenstein and Alessandro Chiesa.

2010–2013 **BA Computer Science**, *University of Cambridge*, UK.

## Preprints

**Quantum Rewinding for IOP-Based Succinct Arguments**.
*Alessandro Chiesa, Marcel Dall'Agnol, Zijing Di, Ziyi Guan and Nicholas Spooner.*

## Publications

2025 **A Zero-Knowledge PCP Theorem**.
*Tom Gur, Jack O'Connor and Nicholas Spooner.*
STOC 2025 (57th ACM Symposium on Theory of Computing)

2024 **An efficient quantum parallel repetition theorem and applications**.
*John Bostanci, Luowen Qian, Nicholas Spooner and Henry Yuen.*
QIP 2024 (27th Annual Conference of Quantum Information Processing, **plenary talk**), STOC 2024 (56th ACM Symposium on Theory of Computing)

**Perfect Zero Knowledge PCPs for #P**.
*Tom Gur, Jack O'Connor and Nicholas Spooner.*
STOC 2024 (56th ACM Symposium on Theory of Computing)
**Featured in Quanta Magazine (4th October 2024).**

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

2023 **On the Necessity of Collapsing for Quantum and Post-Quantum Commitments**.
*Marcel Dall'Agnol and Nicholas Spooner.*
TQC 2023 (18th Conference on the Theory of Quantum Computation, Communication and Cryptography, **Outstanding Paper Prize**), QIP 2023 (26th Annual Conference of Quantum Information Processing; appeared as a poster)

**Speed-Stacking: Fast Sublinear Zero-Knowledge Proofs for Disjunctions**.
*Aarushi Goel, Mathias Hall-Andersen, Gabriel Kaptchuk and Nicholas Spooner.*
Eurocrypt 2023 (42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques)

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

**The Superlinearity Problem in Post-Quantum Blockchains**.
*Sunoo Park and Nicholas Spooner*.
FC 2023 (27th International Conference on Financial Cryptography and Data Security)

2022 **Quantum Rewinding for Many-Round Protocols**.
*Russell W.F. Lai, Giulio Malavolta and Nicholas Spooner*.
TCC 2022 (20th Annual Theory of Cryptography Conference)

**Post-Quantum Zero Knowledge, Revisited (or: How to Do Quantum Rewinding Undetectably)**.
*Alex Lombardi, Fermi Ma and Nicholas Spooner*.
FOCS 2022 (64th IEEE Symposium on Foundations of Computer Science), QIP 2023 (26th Annual Conference of Quantum Information Processing)

**On Succinct Non-Interactive Arguments in Relativized Worlds**.
*Megan Chen, Alessandro Chiesa and Nicholas Spooner*.
Eurocrypt 2022 (41st Annual International Conference on the Theory and Applications of Cryptographic Techniques)

2021 **Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier**.
*Alessandro Chiesa, Fermi Ma, Nicholas Spooner and Mark Zhandry*.
FOCS 2021 (63rd IEEE Symposium on Foundations of Computer Science, **invited to SICOMP special issue**), QIP 2022 (25th Annual Conference of Quantum Information Processing)

**Proof-Carrying Data without Succinct Arguments**.
*Benedikt Bünz, Alessandro Chiesa, Pratyush Mishra, William Lin and Nicholas Spooner*.
CRYPTO 2021 (41st Annual International Cryptology Conference)

2020 **Proof-Carrying Data from Accumulation Schemes**.
*Benedikt Bünz, Alessandro Chiesa, Pratyush Mishra and Nicholas Spooner*.
TCC 2020 (18th Annual Theory of Cryptography Conference)

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

**Efficient Post-quantum SNARKs for RSIS and RLWE and Their Applications to Privacy**.
*Cecilia Boschini, Jan Camenisch, Max Ovsiankin and Nicholas Spooner*.
PQCrypto 2020 (11th International Conference on Post-Quantum Cryptography)

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

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

**Aurora: Transparent Succinct Arguments for R1CS**.
*Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza and Nicholas P. Ward*.
Eurocrypt 2019 (38th Annual International Conference on the Theory and Applications of Cryptographic Techniques), **Journal of the ACM Vol. 69, Issue 2**

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

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

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

2016 **Interactive Oracle Proofs**.
*Eli Ben-Sasson, Alessandro Chiesa and Nicholas Spooner.*
TCC 2016 (14th Theory of Cryptography Conference)

2015 **Fixed-Budget Performance of the (1+1)-EA on Linear Functions**.
*Johannes Lengler and Nicholas Spooner.*
FOGA 2015 (Foundations of Genetic Algorithms XIII)

## Fellowships & Scholarships

Summer 2025 Simons–Berkeley Research Fellowship, *Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation.*

2013-15 ETH Excellence Scholarship

## Service

2024 Co-organiser of NYC Quantum Algorithms, Complexity and Cryptography Day

2022 Co-organiser of UK Crypto Day

### Program committee service

FOCS 2025, Eurocrypt 2025, Latincrypt 2025, CRYPTO 2024, ICALP 2024, TCC 2022, ZKProof4 (2021), TCC 2020, Stanford Blockchain Conference 2020.

## Recent invited talks

2025 **A Zero-Knowledge PCP Theorem**.
Institute for Advanced Studies CSDM Seminar, March 2025

2024-5 **An efficient quantum parallel repetition theorem and applications**.
Cornell Theory Seminar, February 2025
ETH Zürich, July 2024
IRIF, July 2024
INRIA Rennes, July 2024
Korea Institute of Advanced Studies, June 2024
NTT R&D Tokyo, May 2024
UK Crypto Day, June 2024

2024 **Perfect Zero Knowledge PCPs for #P**.
NYC Crypto Day, October 2024

2023-4 **Incrementally-verifiable computation from polynomial oracles**.
EPFL COMPSEC-SPRING Lunch Seminar, July 2024
Columbia Theory Seminar, October 2023

2022 **Efficient zero-knowledge proofs for disjunctions**.
PROOFS@BICI (Bertinoro), July 2022
University of Maryland, September 2022

2022 **Post-quantum cryptographic proofs**.
The Multiple Facets of Quantum Proofs (STOC affiliated workshop), June 2022.

## Teaching

| | |
|---|---|
| Spring 2025 | **CS 4813: Quantum Computing**, Cornell University. |
| Fall 2024 | **CS 6814: Probabilistic Proofs**, Cornell University. |
| Spring 2024 | **CSCI-UA.0480-074: Quantum Computing**, NYU, (undergraduate). |
| Fall 2023 | **CSCI-GA.3033-103: Quantum Computing**, NYU, (graduate). |
| Spring 2023 | **CS419/939: Quantum Computing**, University of Warwick. |
| Spring 2022 | **CS419/939: Quantum Computing**, University of Warwick. |

## Outreach

| | |
|---|---|
| 29 Jan 2020 | **ZKPodcast**, *Episode 114: Exploring the Fractal transparent SNARK construction*. |