Ertem Nusret Tas

nusrettas1996@gmail.com | +1 (646) 323-7949 | nusret1996.github.io

Education

2019–2025	**Stanford University** — Ph.D., Electrical Engineering. Advisors: Dan Boneh, David Tse
2018–2019	**Massachusetts Institute of Technology** — M.Eng., Electrical Engineering and Computer Science. Advisor: Eytan Modiano
2015–2018	**Massachusetts Institute of Technology** — B.S., Electrical Engineering and Computer Science; Minor in Economics. GPA: 5.0/5.0

Industry Experience

Jun 2025 -	**a16z Frontier (formerly Crypto) Research** — Research Associate	New York, NY
Jun-Aug 2023	**a16z Crypto Research** — Research Intern	New York, NY
Jun-Sept 2022	**Babylon Labs** — Intern	Stanford, CA
Jun-Sept 2021	**Celestia (LazyLedger)** — Intern	Stanford, CA
Jun-Aug 2018	**Apple** — Intern	Austin, TX
Jun-Aug 2017	**NetApp** — Intern	Research Triangle Park, NC
May-Aug 2016	**Linear Technology** — Intern	North Chelmsford, MA

Teaching

2026	**Lecturer** (guest lecture) — CSCI-Cryptocurrencies and decentralized ledgers (GA.3033-078), NYU
2022–2023	**Lecturer** (guest lectures) — Cryptocurrencies and Blockchain Technologies (CS 251), Stanford
2023	**Teaching Assistant** — Information Theory (EE 276), Stanford
2018	**Teaching Assistant** — Mathematics for Computer Science (6.042J), MIT

Publications

† *equal contribution and listed alphabetically.* ‡ *listed alphabetically.*

Preprints / ePrints

[1] I. Abraham‡, A. Kate‡, A. Partap‡, and E.N. Tas‡. "Lattice Bingo: Asynchrony and One-Shot Adaptivity in Verifiable Secret Sharing via Erasure Code Commitments". ePrint:2026/2432. Oct. 2026.

[2] A. Frolov‡, A. Partap‡, M. Resnick‡, and E.N. Tas‡. "Weighted Batch Threshold Encryption with Efficient DKG". ePrint:2026/2053. September. 2026.

[3] M. Kelkar, E.N. Tas, M. Bahrani, and T. Roughgarden. "Designing Incentives for Responsive Consensus Protocols". ePrint:2026/1234. June 2026.

[4] J. Liu‡, A. Rubinstein‡, E. N. Tas‡, S. M. Weinberg‡, and Q. Zhang‡. "Single-Item Auctions with a Monopolist Intermediary". arXiv:2605.21934. May. 2026.

[5] G. Fuchsbauer‡, P. Garimidi‡, G.-V. Policharla‡, M. Resnick‡, and E. N. Tas‡. "Non-Delegatable Commitments". ePrint:2025/2039. Nov. 2025.

[6] D. Boneh‡, E. Laufer‡, and E. N. Tas‡. "Threshold Batch Identity-based Encryption without Epochs". ePrint:2025/1254. July 2025.

[7] Y. Efron† and E. N. Tas†. "Dynamically Available Common Subset". ePrint:2025/016. Jan. 2025.

[8] X. Dong‡, O. S. Thyfronitis Litos‡, E. N. Tas‡, D. Tse‡, R. L. Woll‡, L. Yang‡, and M. Yu‡. "Bitcoin Staking". arXiv:2408.01896. Aug. 2024.

[9] E. N. Tas, J. Adler, M. Al-Bassam, I. Khoffi, D. Tse, and N. Vaziri. "Accountable Safety for Rollups". Presented at: *Science of Blockchain Conference (SBC'22)*. arXiv:2210.15017. Oct. 2022.

[10] J. Neu†, E. N. Tas†, and D. Tse†. "Snap-and-Chat Protocols: Systems Aspects". arXiv:2010.10447. Sept. 2020.

Conference / Refereed Papers

[11] I. Abraham‡, K. Nayak‡, L. Ren‡, and E. N. Tas‡. "Synchronous BFT with Provability and Fast Path for the Age of Blockchains". To appear: *IEEE S&P '27*. ePrint:2026/639. April. 2026.

[12] G. Fuchsbauer‡, P. Garimidi‡, J. Neu‡, G.-V. Policharla‡, M. Resnick‡, and E. N. Tas‡. "Doubly Aggregatable Signatures". In: *ACM CCS'26*. ePrint:2026/1042. May. 2026.

[13] D. Boneh[‡], R. Nema[‡], A. Roy[‡], and E. N. Tas[‡]. "Efficient Batch Threshold Encryption Using Partial Fraction Techniques". In: *CRYPTO'26*. ePrint:2026/674. April. 2026.

[14] Y. Efron[‡], J. Neu[‡], L. Ren[‡], and E. N. Tas[‡]. "Optimal Good-Case Latency for Sleepy Consensus". In: *Eurocrypt 2026*. arXiv:2510.06023. Oct. 2025.

[15] J. Komatovic[‡], A. Lewis-Pye[‡], J. Neu[‡], T. Roughgarden[‡], and E. N. Tas[‡]. "From Permissioned to Proof-of-Stake Consensus". In: *Advances in Financial Technologies (AFT'25)*. arXiv:2506.14124. Aug. 2025.

[16] R. Sarenche[†], E. N. Tas[†], B. Monnot, C. Schwarz-Schilling, and B. Preneel. "Commitment Attacks on Ethereum's Reward Mechanism". In: *IEEE European Symposium on Security and Privacy (Euro S&P'25)*. arXiv:2407.19479. July 2024.

[17] S. Sridhar[‡], E. N. Tas[‡], J. Neu, D. Zindros, and D. Tse. "Consensus Under Adversary Majority Done Right". In: *Financial Cryptography and Data Security (FC'25)*. arXiv:2411.01689. Nov. 2024.

[18] E. N. Tas[‡], D. Tse[‡], and Y. Wang[‡]. "A Circuit Approach to Constructing Blockchains on Blockchains". In: *Advances in Financial Technologies (AFT'24)*. arXiv:2402.00220. Jan. 2024.

[19] E. N. Tas, I. A. Seres, Y. Zhang, M. Melczer, M. Kelkar, J. Bonneau, and V. Nikolaenko. "Atomic and Fair Data Exchange via Blockchain". In: *ACM CCS'24*. ePrint:2024/418. (Distinguished Paper Award). Mar. 2024

[20] J. Neu[‡], E. N. Tas[‡], and D. Tse. "Short Paper: Accountable Safety Implies Finality". In: *Financial Cryptography and Data Security (FC'24)*. arXiv:2308.16902. Aug. 2023.

[21] E. N. Tas, D. Tse, L. Yang, and D. Zindros. "Light Clients for Lazy Blockchains". In: *Financial Cryptography and Data Security (FC'24)*. arXiv:2203.15968. Mar. 2022.

[22] F. D'Amato[‡], J. Neu[‡], E. N. Tas[‡], and D. Tse[‡]. "No More Attacks on Proof-of-Stake Ethereum?" In: *Financial Cryptography and Data Security (FC'24)*. arXiv:2209.03255. Sept. 2022.

[23] E. N. Tas and D. Boneh. "Vector Commitments with Efficient Updates". In: *Advances in Financial Technologies (AFT'23)*. arXiv:2307.04085. July 2023.

[24] S. Agrawal, J. Neu, E. N. Tas, and D. Zindros. "Proofs of Proof-of-Stake with Sublinear Complexity". In: *Advances in Financial Technologies (AFT'23)*. arXiv:2209.08673. Sept. 2022.

[25] E. N. Tas and D. Boneh. "Cryptoeconomic Security for Data Availability Committees". In: *Financial Cryptography and Data Security (FC'23)*. arXiv:2208.02999. Aug. 2022.

[26] E. N. Tas, D. Tse, F. Gai, S. Kannan, M. A. Maddah-Ali, and F. Yu. "Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities". In: *IEEE S&P'23*. arXiv:2207.08392. July 2022.

[27] J. Neu[†] and E. N. Tas[†]. "Two Attacks on Proof-of-Stake GHOST/Ethereum". In: *Workshop on Developments in Consensus (ConsensusDay'22)*. arXiv:2203.01315. Mar. 2022.

[28] C. Schwarz-Schilling, J. Neu, B. Monnot, A. Asgaonkar, E. N. Tas, and D. Tse. "Three Attacks on Proof-of-Stake Ethereum". In: *Financial Cryptography and Data Security (FC'22)*. arXiv:2110.10086. Oct. 2021.

[29] J. Neu[†], E. N. Tas[†], and D. Tse[†]. "The Availability-Accountability Dilemma and its Resolution via Accountability Gadgets". In: *Financial Cryptography and Data Security (FC'22)*. arXiv:2105.06075. May 2021.

[30] J. Neu[†], E. N. Tas[†], and D. Tse[†]. "Ebb-and-Flow Protocols: A Resolution of the Availability-Finality Dilemma". In: *IEEE S&P'21*. arXiv:2009.04987. Sept. 2020.

[31] A. Dembo[‡], S. Kannan[‡], E. N. Tas[‡], D. Tse[‡], P. Viswanath[‡], X. Wang[‡], and O. Zeitouni[‡]. "Everything is a Race and Nakamoto Always Wins". In: *ACM CCS'20*. arXiv:2005.10484. May 2020.

Thesis

[32] E. N. Tas. "Economic Security and Scalability in Decentralized Systems". Ph.D. Dissertation, Stanford University, 2025.

[33] E. N. Tas. "Coflow Scheduling in Data Center Networks". M.Eng. Thesis, MIT, 2019.

Invited Talks

[34] E. N. Tas. "Batch Decryption without Epochs and its Application to Encrypted Mempools". CMU × LayerZero Crypto Seminar. Oct. 2025.

[35] E. N. Tas. "Optimal Security in a Multi-chain World". Yale Applied Cryptography Laboratory Seminar. Feb. 2025.

[36] E. N. Tas. "Atomic and Fair Data Exchange via Blockchain". The Science of Blockchain Conference 2024. Aug. 2024

[37] E. N. Tas. "Cryptoeconomic Security for Data Availability Committees". a16z Crypto Research Talk. Feb. 2023.

[38] E. N. Tas. "Accountable Safety for Rollups ". The Science of Blockchain Conference 2022. Aug. 2022

[39] E. N. Tas. "Light Clients for Lazy Blockchains". Modular Summit 2022. Jun. 2022.

[40] E. N. Tas. "Everything is a Race and Nakamoto Always Wins". Decrypto Seminar. Apr. 14, 2021. (Video)

Honors & Awards

- Silver medalist, International Physics Olympiad (IPhO) 2014.
- Ranked 1st among ~2M participants, University Entrance Exam of Turkey.
- ACM CCS 2024 Distinguished Paper Award ("Atomic and Fair Data Exchange via Blockchain").
- Finalist, Meta PhD Research Fellowship (Blockchain & Cryptoeconomics), 2022.
- Winner, Niantic Augmented Reality Prize at HackMIT 2018.
- Landsman Undergraduate Research & Innovation Scholar, MIT SuperUROP (2016–2017).

Service & Leadership

Aug 2024	**Science and Engineering of Consensus 2024** — Workshop Organizer	New York, NY
2022–2024	**Information Systems Lab Colloquium** — Organizer	Stanford, CA
2016–2017	**Gordon MIT Leadership Program** — Gordon Engineering Leader	Cambridge, MA
2016–2017	**MIT Turkish Student Association** — President	Cambridge, MA
2018–2019	**MIT Tau Beta Pi (TBP)** — Secretary & Community Service Chair	Cambridge, MA
2018–2019	**MIT Eta Kappa Nu (HKN)** — Secretary	Cambridge, MA