I view research as a social endeavor. This takes two forms: 1) Research is a fun social activity. 2) Research is done within a larger sociotechnical environment and should be for society's betterment.

While I try to fit all of my research into *both* of these categories, I have also taken two major research directions to fulfill each intention. 1) Complexity Theory asks profound philosophical questions and has compelling narratives about the nature of computation and about which problems' solutions may be provably beyond our reach during our planet's lifetime. Researching, teaching, and mentoring on this field's stories is one my favorite social activities. 2) Algorithmic Fairness' questioning of how algorithms further cement and codify systems of oppression in the world has impacts that are enormously far-reaching both in current global problems and in the nature of future ones. This field is in its infancy and deciding its future and impact with intention is simultaneously exciting and frightening but, above all, of absolute necessity.

Complexity Theory and Cryptography

Understanding the foundations of Cryptography is understanding the foundations of Hardness. Complexity Theory studies the nature of computational hardness – i.e. lower bounds on the time required in solving computational problems – not only to understand what is difficult, but to understand the utility hardness offers. By hiding secrets within 'structured hardness,' Complexity Theory, only as recently as the 1970s, transformed the ancient ad-hoc field of Cryptography into a science with rigorous theoretical foundations. But *which* computational hardness can we feel comfortable basing Cryptography on?

My research studies a question foundational to Complexity Theory and Cryptography:

Does Cryptography's existence follow from $\mathsf{P} \neq \mathsf{NP}$?

P is the class of problems computable in polynomial time and is qualitatively considered the set of 'easy' problems, while NP is the class of problems whose solutions, when obtained, can be *checked* as correct in polynomial time. NP thus captures the computational problems that could be considered of practical interest, lest we wouldn't even know a correct solution when saw it. Since it seems that it should sometimes be harder to *find* solutions than to *verify* them, it is widely believed that $\mathsf{P} \neq \mathsf{NP}$ and resolving this is the largest open problem in Computer Science and one of the seven Clay Millennium "million-dollar" problems in mathematics. Further, $\mathsf{P} \neq \mathsf{NP}$ is the weakest possible assumption on which Cryptography might follow from, intuitively since you must be able to *check* that you have correctly decoded an encrypted message.

While most of Cryptography is based on the assumptions of the hardness of *specific* problems, basing Cryptography on $\mathsf{P} \neq \mathsf{NP}$ is no longer cherry-picked but instead achieves a structural theorem relating the the existence of Cryptography to the hardness of a natural *class* of problems. This would show that NP's problems lack structure that can be exploited for attaining fast algorithms yet retain enough structure to accomplish Cryptography, giving us a window into the nature and flexibility of the type of hardness within one of the most natural and studied complexity classes. My work aims to make progress towards, define variants of, and show barriers to basing Cryptography on $\mathsf{P} \neq \mathsf{NP}$.

Past Work. My work uses the nascent field of Fine-Grained Complexity Theory to open new directions on this long-studied foundational question. By studying "Hardness within P" (see [37, 38]) and the connections of problems computable in, say, n^2 time versus n^3 time, Fine-Grained Complexity addresses the *practical* efficiency of problems. However, while this more *quantitative* approach addresses practical hardness problem-by-problem, we lose connection to key *qualitative* claims of classical Complexity Theory such as the general ability to hide secrets (Cryptography), the ability to show that a world where we have access to randomness is no more powerful computationally than a deterministic one (Derandomization), and the ability to transform a problem that is hard in the worst-case scenario into one that is hard almost always (Hardness Amplification).

My work shows that these connections can be recovered and that the problem-specific claims of Fine-Grained Complexity Theory cannot exist in a vacuum without ramifications to structural Complexity Theory.

• **Hardness Amplification:** My work [4] shows how to take core Fine-Grained problems believed to be hard to compute in the worst-case and, by interpolating the problem's input-output relation with a low-degree multilinear extension over a finite field, create a new function that is now moderately hard *on all but a small fraction* of the problem's instances (this uses the idea that *if you could* quickly solve this low-degree polynomial on more than a small fraction of its inputs, then you could interpolate the rest and thus solve it *on all inputs*, including for the original problem in the worst-case). This sort of 'average-case hardness' is *necessary* for Cryptography since Cryptographic objects should be secure almost always and not only if the adversary is unlucky and receives a worst-case instance. Our low-degree multilinear framework has spawned many works in the average-case hardness of fine-grained problems and in delegating computation – e.g. [1, 15, 16, 17, 18]. By achieving average-case hardness within the Fine-Grained world, we use this as a stepping stone to achieve both Cryptographic primitives and Derandomization.

- **Cryptography:** Introduced in [13] to combat spam and now serving as the heart of many cryptocurrencies, Proofs of Work (PoWs) ask a fundamental question about hardness: Can you *prove* that you expended a certain amount of computational work? We obtain the first PoWs from worst-case complexity assumptions, thus finally shifting them from a heuristic idea to a mathematically grounded Complexity Theoretic object. [5]. Most importantly, we show that these PoWs follow from strengthenings of $\mathsf{P} \neq \mathsf{NP}$, including from the Strong Exponential Time Hypothesis (SETH): Whereas $\mathsf{P} \neq \mathsf{NP}$ is know to be equivalent to a specific problem in NP requiring more than polynomial time [12, 25], SETH states that it requires *exponential* time. Thus, our work not only gives the first PoWs from worst-case assumptions, we give the first Cryptographic objects that follow from a worst-case assumption that is a natural strengthening of $\mathsf{P} \neq \mathsf{NP}$.
- **Derandomization:** We achieve complexity-theoretic Pseudorandom Generators (PRGs) from the core assumptions of Fine-Grained Complexity [11]. These objects are sufficient to *derandomize* algorithms [29], thus showing how a deterministic world may be just as computationally powerful as one where we have free access to true randomness. Our results thus not only connections the resource-centric coarse-grained study of derandomization to the problem-centric hardness of Fine-Grained Complexity, but improves over all previous derandomizations shown from algorithmic hardness assumptions [9, 22, 36]. Further, complexity-theoretic PRGs are weakened versions of Cryptographic PRGs, which are *equivalent* to attaining secret-key Cryptography. Thus, this can be viewed as showing that from Fine-Grained assumptions including from the natural strengthening of $\mathsf{P} \neq \mathsf{NP}$, SETH, we get progress towards secret-key Cryptography.

Future Work. I propose to progress towards, define variants of, and show barriers to and consequences of basing Cryptography on $\mathsf{P} \neq \mathsf{NP}$.

- **Fine-Grained Cryptography:** Beyond the PoWs we achieve in [5], common Cryptographic abilities such as encrypting messages may also be desired. Towards this end, my work [4] introduced the concept of Fine-Grained Cryptography which should be *moderately* secure (hard for n^k time adversaries for some k instead of being super-polynomially hard) and gives definitions of the core objects needed to begin realizing it. This has already inspired the works of [24] and [10] which make progress towards Fine-Grained public-key Cryptography and Fine-Grained secure computation, respectively.

Since Fine-Grained Cryptography is weaker than traditional Cryptography, it may be a form of hiding secrets that *is* achievable from Fine-Grained assumptions and SETH even if traditional Cryptography isn't! But beyond this, moderately hard Cryptography is a qualitatively different object, useful for cases in which it is sufficient for the level of security to simply be prohibitively inconvenient to break yet still breakable. This can be useful in the case of private but not very sensitive data so that a grounded quantitative notion of security remains, but if the owner's secret key is lost or stolen by malicious ransomware the personal data is still recoverable (similar to the security a car's locks provide while being weak enough to not forfeit an entire car if the keys are locked inside). As this area is unexplored and mostly deals with the simple combinatorial problems of Fine-Grained Complexity, there are many directions to be explored with students.

- **Barriers:** One of the trademark qualities of Complexity Theory is its abundance of impossibility and barrier results, proving that certain proof techniques are impossible to achieve a desired theorem or would have to first prove results we either don't believe or seem far beyond our current reach. In particular, there is a long line of research showing barriers to achieving Cryptography from $\mathsf{P} \neq \mathsf{NP}$ – e.g. [2, 8, 14].

The 'flavor' of these barriers, however, are all of the form that a *specific standard set of proof techinques* achieving the goal would yield consequences that we *don't* believe are true. I am in ongoing work to instead show that *any* proof techniques that lead to "$\mathsf{P} \neq \mathsf{NP} \Rightarrow$ Cryptographic PRGs" would result in circuit lower bounds that we've yet to prove but *believe to be true.* For example, we can currently show that "$\mathsf{P} \neq \mathsf{NP} \Rightarrow$ Cryptographic PRGs" would imply that NP is not computable by polynomial size circuits *or* P is hard for *any* fixed polynomial, n^k, size circuits. Both consequences are believed and this shows that connecting $\mathsf{P} \neq \mathsf{NP}$ to Cryptography would imply that at least one of them must be true! Disjunctions of circuit bounds as a barrier is similar to [23] but this would be the first result of its kind about Cryptography.

Algorithmic "Fairness"

Algorithms that predict recidivism – i.e. whether a person awaiting trial for a suspected crime will commit further crimes if not detained – have been consistently exposed as being badly biased in inaccuracy against black people, resulting in [3] famously exposing the widespread COMPAS algorithm. This is a notorious example in Algorithmic Fairness and creating more "Fair" recidivism predictors is commonly used as motivation for new work in the field. However, this task is necessarily written from the perspective of the jailer. Was this the intended outcome of the "watchdog" effort of exposing COMPAS? Algorithms, even ones attempting "Fairness," codify and legitimize the systems using them, and thus the main question of this nascent field is this: What should our *role* be as Algorithmic Fairness researchers?

Continuing Work: "Fairness." My entrance into Algorithmic Fairness was *both* as a Computer Scientist and as a member of the Queer, Trans, and Person of Color (POC) community. From this intersection, I had reservations that an abstract notion of a "Fair" algorithm would not be portable to multiple social contexts and runs the risk of harming my communities while still allowing companies a "Fairness" stamp of approval. I entered the field to make sure my community and their concerns and values were reflected.

After participating heavily in the Simons Institute at UC Berkeley's 2019 Summer program on Algorithmic Fairness, I found that many of my reservations were directly reflected in numerous critiques from this past year – e.g. [7, 19, 20, 21, 34]. I thus began collaborating with an interdisciplinary group of graduate students from Computer Science, Medicine, and Philosophy across multiple universities to create and organize a workshop for the upcoming ACM Fairness, Accountability, and Transparency (FAT*) 2020 Conference.

The workshop's target audience is Fairness researchers who are troubled by the emerging critiques but are unsure how to begin addressing them. Our workshop argues that, beyond moving from a *multi*discplinary field to an *inter*discplinary one, we should seek guidance beyond academic disciplines altogether. In particular, we guide the audience through praxis-centered methods from Community Organizing and begin a dialogue of grounding our emerging field in Community Organizing principles and methodologies.

Using the insights we gained in the workshop's preparation, we are in ongoing work to be submitted to FAT* 2021 detailing a restructuring of Algorithmic Fairness to more explicitly address the question of what our *role* should be as "Fairness" researchers. We introduce the Discriminatory and Liberatory Algorithms (DLA) framework which splits the type of work to be done in Algorithmic Fairness into two categories:

- **Algorithms of Discrimination:** This is exclusively "watchdog" work, where 1) Fairness researchers relabel their abstract attempts to define "Fairness" (which can be dangerously misleading) as the building of an increasingly sophisticated suite of statistical tools that formalize certain types of discrimination, and 2) interdisciplinary efforts are taken to use these statistical tools to expose algorithmic discrimination in the real world. The end goal of this category is to gather enough evidence of algorithmic discrimination and to develop enough language so that policy change can be argued for against discriminatory practices.
- **Algorithms of Liberation:** This area considers how and where algorithms can be used to put power and autonomy into the hands of marginalized groups. This area is *problem-driven*, where abstract and portable notions of "Fair algorithms" are discarded in favor of finding a specific need in the world by a specific population in a specific context at a specific point in time and then undertaking an interdisciplinary effort using mathematical tools as well as anthropological ones and involving community feedback and guidance to craft an algorithm for this need. The utility of this specific algorithm, then, is justified with a holistic argument that has both quantitative and qualitative reasoning interlaced.

This framework, thus, is not just a renaming of different objectives of the field but attaches methodologies and domain boundaries to its categories. Much of the abstraction, for example, is isolated to developing a suite of statistical tools while all else (including the tools' usage) is done through a sociotechnical lens.

The virtue of the framework is best understood with respect to [34], which outlines a series of "traps" the field of Fairness seems to routinely fall into, including a naming of my fear that abstract notions of "Fairness" can hurt the communities they intend to serve when ported between differing contexts as the "Portability Trap." We argue that the DLA framework aims at the same goal of producing a more just world with respect to algorithm usage while being much less prone to these traps. The "Portability Trap," for example, is mitigated since the only construction of algorithms in this framework is in the Liberatory Algorithms category which is, by design, problem-specific and holistic and so explicitly makes no claims to abstract portability. Another illustrative trap is the "Solutionism Trap" of prematurely presuming that a technological solution to a social problem is required or useful. This reveals a third category:

- **Other Algorithms?:** Our two-pronged categorization does not partition all possible Fairness efforts. Consider developing recidivism prediction algorithms that are *less* discriminatory. This may not fit well into Algorithms of Liberation as the algorithm is for use by the jailer and not the affected population, and is also not a watchdog Discriminatory Algorithms effort. So where does this effort exist in the framework?

By *default*, it doesn't. One could still argue that recidivism predictors continue to exist and that having a less discriminatory one is preferable for the time being as a 'harm reduction' tactic. We welcome these types of nuanced sociotechnical arguments! The key point is that its existence is not *presumed*. Efforts that introduce *technology* into *society* must have their merit *justified* through a *sociotechnical* argument. This allows these projects to exist in this framework while guarding against the Solutionism Trap.

Algorithmic Fairness is in its formative stages and it is crucial to decide how the field will evolve in its methodologies, terminology, politics, conventions, and demographics. I will continue in this ongoing work and further use this lens and the insights gained to consider the similarly sociotechnical Cryptography.

Future Work: "Trust" and "Privacy." When Apple introduced Differential Privacy to its Operating Systems it seemed a step in the right direction, however it was soon shown that the parameters chosen made any claims to privacy very specious [35]. That is, the beguiling *certainty* that a technological guarantee inspires is dangerously at odds with the many normative decisions present in all stages of implementation. It is clear that a normative framework is needed.

Indeed, the work "Is Privacy *Privacy*?" [31] explores the gap between normative and technical meanings of words like "privacy" and calls for a bridging of this gap. One existing attempt is Nissenbaum's Contextual Integrity (CI) [30] which wholly embraces "privacy" as a socially and culturally decided upon norm that is constantly changing. It presents a framework for identifying how data flows through a system and at which points data is being transferred from one entity to another, where a normative judgment of whether that transfer is "appropriately" private is needed. Thus, rather than codifying absolute notions of "privacy" as types of secrecy, it recognizes them to be ever-changing norms on "appropriate" information handling.

However, while CI clarifies a framework for identifying *where* normative decisions should take place, it offers no guidance as to *who* makes these choices. I plan to work across disciplines to construct a framework for deciding who makes these normative decisions and how stakeholders' inputs are incorporated. It should, for instance, be the case that the communities whose data is being operated on should have some say on these decisions. There is much work to do in deciding how to prioritize vulnerable populations, how interests can be incorporated through qualitative means (e.g. using Community-Based Participatory Research methods [28]), and how this problem changes as the populations scales or even becomes global.

Further, with cryptosystems often using a private company as a "trusted third party" and with the strong research push to make fully anonymous cryptocurrencies [6, 27, 33] despite their claimed use in the black market and human trafficking, it is clear that a normative framework for understanding our *role* as Cryptographers is much needed [32]. Social anthropologist Adrienne Mannov has recently called for a Crypto-Anthropology [26] and I am now using both my expertise in theoretical Cryptography and my immersion in its community along with the sociotechnical lens I've gained from both the Queer community and my work in Algorithmic Fairness to collaborate with Mannov to undertake an anthropological study of Cryptography research. We are studying in which ways the core Cryptographic primitives, by mere existence, are inherently political, akin to [39], and in which political and social contexts these notions arose. By understanding the politics these abstract technologies enact on the world and by delineating a list of normative "traps" that the culture of Cryptography research seems to fall into similar to the ones discovered for Algorithmic Fairness [34], we may begin to understand what our *role* has been along with what it should be as Cryptographers.

Conclusion

My work studies both the aesthetics of Pure Mathematics and Complexity Theory as well as the ways in which Engineering and Computer Science are born out of social circumstances which then affect that society in a feedback loop. While foundational in nature, my work leaves many concrete and tractable problems in its wake which, when combined with the freshness of these areas, both ensures that students can begin work with minimal on-boarding and gives many opportunities for interdisciplinary directions to explore.

In Complexity Theory, my longterm goal is to understand the foundations of Cryptography and its relationship to NP. While ambitious, I have already begun novel progress on this front and the emergence of Fine-Grained Complexity seems to be shedding new light onto this old and studied question.

My goals in Algorithmic Fairness might be yet more ambitious: I want to see an Algorithmic Fairness where the researcher demographics reflect the communities that stand to be most affected by the algorithms in question. I believe my framework takes a step in that direction by moving towards research and values that reflect these communities, thus allowing for an environment where new researchers holding identities within these populations will feel comfortable joining.

References

[1] Enric Boix Adserà, Matthew Brennan, and Guy Bresler. The average-case complexity of counting cliques in erdős-rényi hypergraphs. *CoRR*, abs/1903.08247, 2019.

[2] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. On basing one-way functions on np-hardness. In Jon M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 701–710. ACM, 2006.

[3] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. Machine bias: There's software used across the country to predict future criminals. and it's biased against blacks. *ProPublica*, 2016.

[4] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 483–496. ACM, 2017.

[5] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Proofs of work from worst-case assumptions. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part I*, volume 10991 of *Lecture Notes in Computer Science*, pages 789–819. Springer, 2018.

[6] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014*, pages 459–474. IEEE Computer Society, 2014.

[7] Cynthia L. Bennett and Os Keyes. What is the point of fairness? disability, ai and the complexity of justice, 2019.

[8] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. In *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*, pages 308–317. IEEE Computer Society, 2003.

[9] Jin-yi Cai, Ajay Nerurkar, and D. Sivakumar. Hardness and hierarchy theorems for probabilistic quasi-polynomial time. In Jeffrey Scott Vitter, Lawrence L. Larmore, and Frank Thomson Leighton, editors, *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, May 1-4, 1999, Atlanta, Georgia, USA*, pages 726–735. ACM, 1999.

[10] Matteo Campanelli and Rosario Gennaro. Fine-grained secure computation. In Amos Beimel and Stefan Dziembowski, editors, *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*, volume 11240 of *Lecture Notes in Computer Science*, pages 66–97. Springer, 2018.

[11] Marco L. Carmosino, Russell Impagliazzo, and Manuel Sabin. Fine-grained derandomization: From problem-centric to resource-centric complexity. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, volume 107 of *LIPIcs*, pages 27:1–27:16. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[12] Stephen A. Cook. The complexity of theorem-proving procedures. In Michael A. Harrison, Ranan B. Banerji, and Jeffrey D. Ullman, editors, *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, May 3-5, 1971, Shaker Heights, Ohio, USA*, pages 151–158. ACM, 1971.

[13] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147. Springer, 1992.

[14] Joan Feigenbaum and Lance Fortnow. On the random-self-reducibility of complete sets. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, Illinois, USA, June 30 - July 3, 1991*, pages 124–132. IEEE Computer Society, 1991.

[15] Oded Goldreich. On doubly-efficient interactive proof systems. *Foundations and Trends in Theoretical Computer Science*, 13(3):158–246, 2018.

[16] Oded Goldreich and Guy N. Rothblum. Worst-case to average-case reductions for subclasses of P. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:130, 2017.

[17] Oded Goldreich and Guy N. Rothblum. Counting t-cliques: Worst-case to average-case reductions and direct interactive proof systems. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:46, 2018.

[18] Oded Goldreich and Guy N. Rothblum. Counting t-cliques: Worst-case to average-case reductions and direct interactive proof systems. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 77–88. IEEE Computer Society, 2018.

[19] Ben Green. Data science as political action: Grounding data science in a politics of justice, 2019.

[20] Ben Green and Lily Hu. The myth in the methodology: Towards a recontextualization of fairness in machine learning. In *Machine Learning: The Debates workshop at the 35th International Conference on Machine Learning (ICML)*, Stockholm, Sweden, 2018.

[21] Anna Lauren Hoffmann. Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication & Society*, 22(7):900–915, 2019.

[22] Russell Impagliazzo and Avi Wigderson. Randomness vs. time: De-randomization under a uniform assumption. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, pages 734–743. IEEE Computer Society, 1998.

[23] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. In Lawrence L. Larmore and Michel X. Goemans, editors, *Proceedings of the 35th Annual ACM Symposium on Theory of Computing, June 9-11, 2003, San Diego, CA, USA*, pages 355–364. ACM, 2003.

[24] Rio LaVigne, Andrea Lincoln, and Virginia Vassilevska Williams. Public-key cryptography in the fine-grained setting. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*, volume 11694 of *Lecture Notes in Computer Science*, pages 605–635. Springer, 2019.

[25] L. A. Levin. Universal sequential search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.

[26] Adrienne Mannov. A call for crypto-anthropology. MIT Cryptography and Information Security (CIS) Seminar 2019, October 2019. https://www.csail.mit.edu/event/adrienne-mannov-call-crypto-anthropology.

[27] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*, pages 397–411. IEEE Computer Society, 2013.

[28] Darakhshan J. Mir, Yan Shvartzshnaider, and Mark Latonero. It takes a village: A community based participatory framework for privacy design. In *2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2018, London, United Kingdom, April 23-27, 2018*, pages 112–115. IEEE, 2018.

[29] Noam Nisan and Avi Wigderson. Hardness vs. randomness (extended abstract). In *29th Annual Symposium on Foundations of Computer Science, White Plains, New York, USA, 24-26 October 1988*, pages 2–11. IEEE Computer Society, 1988.

[30] Helen Nissenbaum. *Privacy in Context - Technology, Policy, and the Integrity of Social Life.* Stanford University Press, 2010.

[31] Kobbi Nissim and Alexandra Wood. Is privacy privacy? *Philosophical Transaction of the Royal Society A*, 376(2128), 2018.

[32] Phillip Rogaway. The moral character of cryptographic work. *IACR Cryptology ePrint Archive*, 2015:1162, 2015.

[33] Antoine Rondelet and Michal Zajac. ZETH: on integrating zerocash on ethereum. *CoRR*, abs/1904.00905, 2019.

[34] Andrew D. Selbst, Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian, and Janet Vertesi. Fairness and abstraction in sociotechnical systems. In *Proceedings of the Conference on Fairness, Accountability, and Transparency, FAT* 2019, Atlanta, GA, USA, January 29-31, 2019*, pages 59–68. ACM, 2019.

[35] Jun Tang, Aleksandra Korolova, Xiaolong Bai, Xueqiang Wang, and XiaoFeng Wang. Privacy loss in apple's implementation of differential privacy on macos 10.12. *CoRR*, abs/1709.02753, 2017.

[36] Luca Trevisan and Salil P. Vadhan. Pseudorandomness and average-case complexity via uniform reductions. In *Proceedings of the 17th Annual IEEE Conference on Computational Complexity, Montréal, Québec, Canada, May 21-24, 2002*, pages 129–138. IEEE Computer Society, 2002.

[37] Virginia Vassilevska Williams. Hardness of easy problems: Basing hardness on popular conjectures such as the strong exponential time hypothesis (invited talk). In Thore Husfeldt and Iyad A. Kanj, editors, *10th International Symposium on Parameterized and Exact Computation, IPEC 2015, September 16-18, 2015, Patras, Greece*, volume 43 of *LIPIcs*, pages 17–29. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

[38] Virginia Vassilevska Williams. On some fine-grained questions in algorithms and complexity. In *Proceedings of the ICM*, 2018.

[39] Langdon Winner. Do artifacts have politics? *Daedalus*, 109(1):121–136, 1980.