Statement of Purpose

Naman Kumar **Ph.D. Applicant**

I am primarily interested in cryptography and its applications to security. My career goal is to work as a researcher in cryptography. Modern advancements in complexity theory have driven hope that cryptography will become instrumental in yielding power over future systems. In pursuit of this goal, my research interests deal with the foundations of modern cryptography and spearheading the theoretical development of concretely efficient protocols and primitives.

My success in the high-school math Olympiad led to a fascination with solving logical problems. In December 2020, I joined Chennai Mathematical Institute due to its strong curriculum in advanced mathematics. As a double major, I enjoyed the abstraction that math brought to the table but found myself looking for pursuits that applied that theory in clever ways to solve problems of current interest. The grounding in algebra and complexity theory I gained through my coursework drew me toward CS theory and cryptography, one of the few fields that straddles the line between abstraction and applicability.

This semester I took an entirely graduate course load which included Advanced Complexity Theory and a course on Cryptography from Lattices. The detailed study of modern results in computer science such as Dinur's proof of the PCP theorem and NIZK from LWE has left me with a deep appreciation for the tools of complexity theory − the widespread applicability of the constructions developed from such beautiful techniques has convinced me that cryptography is exactly the field I am looking for. While I am broadly interested in exploring all aspects of cryptography, I have worked in two major areas that pique my interest.

Foundations and Verifiable Computing. Over the past year, I have worked with Prof. Chaya Ganesh on low-communication Byzantine Agreement (BA). BA protocols strive to allow systems to achieve consensus on a plan of action even in the presence of adversarial computers. The particular BA protocol we are interested in, [BCG21], uses a signature scheme called SRDS to authenticate messages. In the course of our research, I provided a formal proof that SRDS can also be used to construct succinct, non-interactive cryptographic arguments (SNARGs). Using recently discovered impossibility results, I also determined the relative security of these arguments and analyzed the kind of adversaries they were secure against. My results have given insight into the structure of primitives used in BA and determined the kind of constructions that would be used to achieve it. Our work was showcased at a presentation at the Indian Institute of Science.

My work has allowed me to better understand the problems that distributed systems face and appreciate the effectiveness cryptographic tools bring to the table. Exposure to state-of-the-art research has affirmed that the inherent nature of the problems genuinely appeals to me. A repeated problem I encountered in my research was the question of determining *why* the argument systems we had developed were succinct. A lack of clarity after reading recent results convinced me that provable security results in these fields often arrive after primitives that use them are already being developed (and implemented). Consider results like [CGH04] or [GW11], the subjects of which (the Random Oracle Model and SNARGs) had been widely adopted for decades. Questions like these are constantly lurking around the corner; I am continuing that line of work with Prof. Ganesh and exploring the foundations of probabilistic proofs and their interplay with succinct arguments and witness encryption. More research in the foundations of primitives like obfuscation, zero-knowledge, and proof systems is required to reach the limits of computational soundness.

Secure Multi-party Computation (MPC). My positive experiences with research made me excited to learn more about cryptography, and I was most intrigued by how naturally it arose out of any problem involving adversarial behavior (like BA). I reached out to Prof. Akshayaram Srinivasan at TIFR to learn more about such problems in MPC. After learning about the basic tenets of secure computation, I studied techniques to achieve practical, efficient MPC such as correlation generators, distributed point functions, and compilers to boost semi-honest protocols to maliciously secure protocols. Following some preliminary work on OT extension, we used these ideas in collaboration with Microsoft Research and applied them to private information retrieval (a protocol that allows a client to retrieve data from servers without revealing to the servers what the data is). Our new scheme achieves multi-server PIR with low communication and less client-side processing and guarantees output delivery. We are now working on an implementation (which I am leading) and preparing our results for publication.

Working in MPC has made me a better researcher. MPC involves ideas from many different domains, and the variety of results I read led me to understand how disparate ideas come together naturally in the flow of research. The versatility of this model exudes abstraction, but concretely efficient techniques to realize even basic functionalities such as garbled circuits, OT, or secure computation in the malicious setting are

not well-developed enough to be implemented at a large scale. The privacy-preserving potential of MPC demands further research. I plan to continue my exploration of MPC in graduate school.

Through these and other experiences, I have determined that research is not just something I like, but something I can excel at. Graduate school is the clear step forward. At the end of a Ph.D. I expect to be at the cutting edge of modern developments and solving problems which are relevant to both theoretical cryptography and privacy-protecting systems in the real world.

Applied work. This summer I interned at an organization called xKDR, where I developed tools for Julia Computing. My project proposal to develop statistical infrastructure was accepted to the Julia Summer of Contributions where I worked on packages that enable researchers to empirically analyze the effect of sudden events on data. This work was presented at JuliaCon 2022. I enjoyed developing scientific tools and left with an appreciation for research that holds immediate applications. Building on this, I joined an online reading group run by Prof. Justin Thaler to get up to speed with the latest open-source developments in crypto. After brushing up my theory and programming skills, I am currently interning at Panther Protocol, where my work involves developing libraries for field arithmetic and implementing in-house SNARKs that allow for better inter-blockchain communication.

My work in both open-source and proprietary systems has led to an understanding of the security problems that command-line cryptography can fall into. While it is true that implementations of numerical libraries are still largely academic, I have found that the true performance bottleneck is the raw mathematical infrastructure and the theoretical efficiency of protocols. Working with Brown's wealth of security researchers will allow me to put my ideas to improve current cryptographic infrastructure into action smoothly.

The culmination of my education and work is that I am comfortable with the knowledge and perspective required to do research. My background enables me to grasp new ideas quickly and rigorously. I have also worked as a teaching assistant at CMI and enjoy sharing my knowledge and learning new approaches to problems. My next goal is to expand these boundaries and become a full researcher in computer science − I believe I am ready for a Ph.D. and for contributing to current research.

I wish to continue my studies at Brown University due to its strong computer science department with a diversity of coursework, access to best-in-class labs, renowned faculty, and regular seminars that will help me to mature as a computer scientist. I am particularly interested in working with **Prof. Peihan Miao** on efficient constructions and foundational results in multi-party computation, and I believe that my strong background in the field would make me a great fit for her work. I would also like to work with **Prof. Anna Lysyanskaya** on foundations and privacy-preserving technologies. Brown's success at getting students engaged with research even within the first year would allow me to immediately get settled in accomplishing my goals: I hope to make significant contributions to cryptography and the world.

References

[BCG21] Elette Boyle, Ran Cohen, and Aarushi Goel. Breaking the o(n)-bit barrier: Byzantine agreement with polylog bits per party. In *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing*, PODC'21, page 319–330, New York, NY, USA, 2021. Association for Computing Machinery.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4):557–594, jul 2004.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, page 99–108, New York, NY, USA, 2011. Association for Computing Machinery.