RESEARCH STATEMENT

Akhil Bandarupalli (abandaru@purdue.edu)

I am a researcher in distributed systems and applied cryptography. My work focuses on designing lightweight and practical solutions for building secure systems that enable privacy-preserving computation, distributed ledgers and blockchains, and resource-constrained Cyber-Physical Systems (CPS). My research lies at the intersection of distributed computing and applied cryptography, with a particular emphasis on quantum-safe cryptography.

Background

Distributed systems have seen widespread adoption in mainstream services as well as the emerging Web3, AI, and distributed CPS ecosystems, mainly due to their ability to support large scale applications. Despite their widespread adoption, these systems remain vulnerable to costly outages caused by machine failures and network instability, as well as to cyber attacks that compromise sensitive data and user privacy. Although extensive research has sought to make distributed systems reliable and secure, these solutions typically impose steep performance penalties and undermine scalability, the main advantage of distributed systems. Reliability and security have thus long been perceived as being at odds with scalability and efficiency, limiting the practical adoption of these solutions and giving way to more such breakdowns and breaches. In addition, the impending era of quantum computers and their ability to disrupt the current security apparatus threatens to further compound these challenges.

My research addresses these challenges through the design of Secure Distributed Computing (SDC) protocols, which provide the algorithmic foundations for reliable and secure distributed systems. I design lightweight protocols tailored to real-world deployment conditions, including hardware and network constraints, while carefully considering the resource overhead introduced by various cryptographic and distributed computing primitives. During my Ph.D., my research focused on building (a) Scalable privacy-preserving or Multi-Party Computation (MPC) protocols, and (b) Resource-efficient distributed protocols for Cyber-Physical Systems and cyber physical security. In both domains, my work demonstrated orders of magnitude improvement over prior works at scale, bringing reliability and security substantially closer to practicality while not compromising scalability. In the long term, my vision is to reduce the gap in performance between secure and non-secure systems to the limits dictated by impossibility results, and in some cases, to make security essentially free, in both today's world and in a post-quantum future.

Scalable and Practical Multi-Party Computation

Secure Multi-Party Computation (MPC) enables mutually distrustful parties to jointly compute any function over their private inputs while preserving input confidentiality. MPC is considered a cornerstone of distributed cryptography and privacy-preserving distributed systems, with applications in anonymous communication, private auctions, healthcare analytics, privacy-preserving AI, DeFi, and CPS ecosystems. With increasing adoption of privacy-preserving technologies, systems that can scale to hundreds of parties have seen increased demand, especially in AI, Web3 ecosystems.

However, despite decades of research, the practical impact of MPC has been constrained by the challenges I aim to solve. Most protocols either fail to scale beyond a handful of participants or assume idealized network conditions, rendering them unreliable in real-world deployments. The few protocols built for realistic, asynchronous networks typically incur prohibitive resource overhead, forcing a trade-off between scalability, reliability, and privacy , hindering the adoption of this critical technology, and ultimately forcing users to compromise on privacy.

These scalability challenges in MPC largely arise from the high cost of scaling cryptography. For instance, early works in asynchronous MPC relied on information-theoretic (IT) cryptography, which incurred extremely high communication overheads, amounting to gigabytes of data transfer even for as few as $n = 10$ participants [5]. To reduce these costs, subsequent protocols adopted public-key cryptography based on stronger hardness assumptions [7, 6]. While this improved communication efficiency compared to IT protocols, it introduced a new bottleneck: computation. Public-key protocols often require hours of computation at $n = 100$ participants, mainly from cryptographic operations. Looking ahead, the impending era of quantum computers threatens to make this problem even worse, as public-key tools are expected to be roughly two orders of magnitude slower in the post-quantum era, further degrading efficiency and scalability.

Lightweight Cryptography My research directly addresses this computational bottleneck by designing a new class of SDC protocols built using lightweight cryptography, such as symmetric encryption and hash functions. These tools are two orders of magnitude faster than public-key alternatives and are also expected to be secure against quantum adversaries. However, they lack the algebraic structure of public-key-based systems, often leading to higher communication costs to guarantee security. We address this limitation by coupling lightweight cryptography with novel distributed computing algorithms and tame the increase in communication. This design principle allows the computational efficiency of lightweight tools to dominate, making secure protocols far more scalable and practical.

My research has produced an efficient, distributed privacy-preserving computation platform through HashRand [1], a secure randomness beacon, and Velox [2], a multi-party computation protocol that offers Fairness. In both works, contrary to the existing trend in SDC research, we prioritized computational efficiency at the expense of slightly higher communication cost, an $O(\log(n))$ factor increase in HashRand and a constant factor increase in Velox. This principle yielded an order of magnitude improved performance for HashRand and two orders of magnitude for Velox (Check fig. 1). In addition to the difference in computation costs between lightweight and public-key cryptography, the improvement in communication infrastructure in the past few decades also contributed to this overall speedup.

Building on these works, we implemented an anonymous broadcast service that allows users to send messages while remaining fully anonymous, supporting real-world applications such as allegation escrows, whistleblowing, and censorship resistance. Anonymity is difficult to guarantee because it requires private computation over many messages, because of which prior systems often settled for weaker variants that could be broken with modest effort. Our techniques achieved strong anonymity with real-time, sub-second broadcast latencies and performance comparable to insecure alternatives. Another cherry on top is that our techniques and systems will last through the impending era of quantum computers because of lightweight cryptography's quantum resilience.

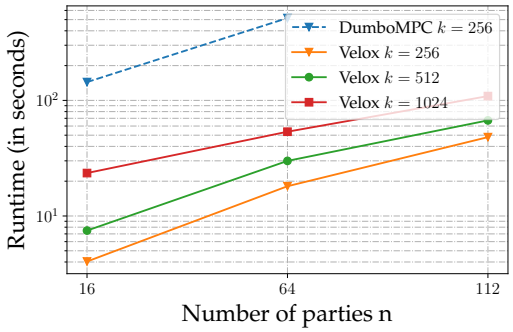

Figure 1: Latency of Anonymous Broadcast of k messages implemented using Velox in comparison with the prior best work DumboMPC [6] based on public-key cryptography. Velox achieves a two orders of magnitude improvement, mainly due to its computational efficiency.

Resource-Efficient Distributed Computing for Cyber-Physical Systems

Cyber-Physical Systems (CPS) have seen rapid adoption in domains such as the Internet of Things, autonomous vehicles, digital agriculture, and battlefield applications like drone swarms. Here, security and reliability failures are not merely digital - they have direct, often critical, consequences in the physical world. Additionally, these systems are also often deployed at a massive scale in remote environments where they must operate on finite battery reserves and over low-bandwidth, unreliable ad-hoc networks, which further amplifies these challenges in reliability. These severe resource constraints make traditional security solutions prohibitively expensive, further intensifying the conflict between security and scalability.

Despite their growing scale, most CPS still depend on centralized points of failure, such as command-and-control centers. While migrating to SDC protocols could in principle improve reliability, existing solutions remain impractical. Their reliance on expensive public-key cryptography makes them too resource-hungry, consuming excessive energy and rapidly depleting battery reserves. Lightweight cryptographic primitives may reduce computational cost but often do so by increasing communication. Unlike in conventional distributed systems where this trade-off succeeded, the fragile communication infrastructure in the CPS setting cannot tolerate this high communication cost. For these reasons, I first try to build reliability and adopt fundamental concepts of distributed systems in such systems and only aim for advanced and more expensive properties like privacy in the subsequent stages.

My research directly confronts these challenges by developing novel, resource-efficient protocols that are fundamentally tailored for the unique constraints of CPS. My approach uses approximate computation techniques like approximate agreement protocols, which strategically sacrifice negligible amounts of agreement precision in exchange for significant gains in energy and network efficiency. While this concept is not new, prior works in approximate agreement have impractically high (cubic) communication costs, hindering its use in scalable CPS. My contributions overcome this barrier.

Efficient Approximate Agreement for Oracles Our work Delphi [3] tackled this problem in the context of distributed oracles, where sensors must agree on real-world state values, such as the price of Bitcoin or the geo-location of an object. Delphi introduced an additional dimension of approximation called accuracy, defined as the distance between the output and the true state value. By jointly approximating precision and accuracy, Delphi achieved only quadratic communication cost, significantly reducing resource overhead. Additionally, we tuned precision and accuracy parameters based on data-driven analysis of their practical impact on two applications: cryptocurrency price feeds and drone swarms geo-locating objects. Experiments on an embedded device testbed showed an order-of-magnitude improvement in energy and bandwidth consumption over the prior best SDC protocol, with only negligible impact on application-level guarantees in both applications.

Scalable CPS using Voronoi Diagrams Our work SensorBFT [4] introduces a new approach based on techniques in computational geometry to address the challenge of scalable area monitoring in applications like digital agriculture or wide-area surveillance. In these systems, sensors with limited range must collaboratively monitor a large area. SensorBFT employs k-order Voronoi diagrams to divide the area among sensors, guaranteeing that every point is monitored by its k-closest sensors. This approach reliably monitors the entire area while tolerating k/3 sensor failures. By integrating this technique with the resource-efficient agreement methods from Delphi, SensorBFT provides a scalable and reliable system for distributed sensing in real-world CPS environments.

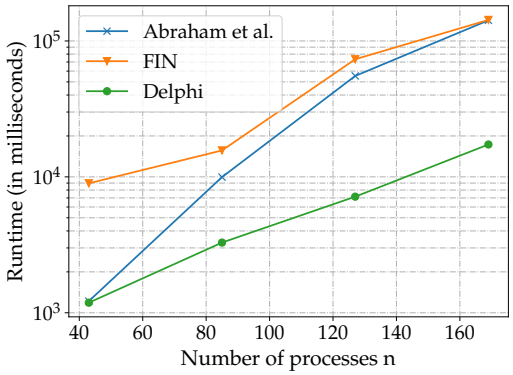

Figure 2: Latency of Oracle agreement with varying number of parties in an embedded device testbed. Delphi achieves an order of magnitude improvement over prior works [8, 9], mainly due to its resource efficient execution.

Current and Future Work

Overcoming Computation and Communication Bottlenecks in large scale MPC

My future research agenda builds directly on my prior work, aiming to address the computation and communication bottlenecks currently limiting deployment of MPC at scale. Additionally, on top of conventional security guarantees like security with abort and fairness, I aim to build practical MPC with Guaranteed Output Delivery (GOD), which ensures parties always output even with malicious parties. MPC with GOD offers a greater degree of reliability and is considerably more expensive than Fairness or Security with Abort. I plan to accommodate this cost by focusing my efforts on accelerating computation and improving communication costs.

Hardware Acceleration for Post-Quantum MPC Despite advances in protocol efficiency, the computational cost of privacy-preserving distributed systems still scales linearly with the number of participants in the system. This burden, driven by lightweight cryptographic operations and Galois field arithmetic operations, becomes prohibitive for larger applications such as privacy-preserving AI with large models. Even with lightweight cryptography, computation remains a key bottleneck to realizing practical large-scale MPC in conventional CPU-based implementations.

To address this challenge, I plan to explore hardware acceleration using parallelized platforms like GPUs. While prior work has used GPUs to accelerate MPC, these solutions are limited to a handful of parties and employ cryptographic techniques that are incompatible with the large-scale, multi-party setting. Hence, their methods of employing GPUs for accelerating computation do not apply to this setting. In the future, I plan to utilize GPUs to specifically accelerate computationally intensive operations in MPC. Concretely, my plan contains three parts.

1. **Custom Kernels**: Developing optimized kernels for Galois field arithmetic essential for secret sharing and circuit evaluation.
2. **Protocol Co-Design**: Designing round-efficient protocols that minimize GPU-CPU data transfer overhead by keeping computation on the GPU.
3. **Post-Quantum Primitives**: Leveraging the inherent parallelism of lightweight, post-quantum friendly primitives (like hash functions), which are far easier to accelerate on GPUs than their public-key counterparts.

Gracefully scaling communication Beyond computation, communication costs in our described MPC protocols also grow linearly with the number of participants, creating another scalability barrier. Prior works proposed constant-communication protocols, but these either rely on expensive public-key cryptography, especially costly in a post-quantum setting, or incur large constants, making them practical only at very large scales (thousands of parties). My research seeks to reduce these constants using lightweight cryptography, enabling more efficient constant-communication protocols without sacrificing practicality.

Ultimately, by coupling hardware-accelerated computation with constant-overhead communication, my research aims to bring the performance of reliable and post-quantum secure MPC significantly closer to practicality, paving the way for their widespread real-world deployment.

Building next generation of Reliable Cyber-Physical Systems

An integral part of my research plan focuses on enabling the next generation of reliable and secure Cyber-Physical Systems. My approach involves two key directions: (a) Efficient SDC protocols for accommodating multi-dimensional data from

sensors, and (b) Integrating the dynamic mobility of highly mobile CPS, such as drone swarms, with techniques from fault tolerance and computational geometry to create robust and self-sustaining systems.

Efficient Convex Agreement for Decentralized Machine Learning Another thrust of my research explores the foundations of Decentralized Machine Learning (DML) protocols that allow multiple parties to collaboratively train models without relying on a central coordinator. Such systems play a crucial role in enabling autonomous CPS applications like the Internet of Vehicles and drone swarms, where local data collected by multiple agents must be aggregated for joint decision-making.

A key technical bottleneck in these systems is the convex agreement problem, which requires participants to agree on an output within the convex hull of their inputs. Existing approaches either incur exponential computational cost in the number of parties or decompose multi-dimensional problems into independent one-dimensional subproblems, thereby losing inter-dimensional correlations and often producing outputs outside the convex hull. I plan to address this challenge by employing randomness in combinatorial geometry and by adapting approximation principles from my prior work to design efficient and practical convex agreement protocols. My end goal is to develop scalable Decentralized ML frameworks that serve as viable decentralized alternatives to the currently centralized Federated Learning ecosystem.

Dynamic and Reliable Swarming in CPS The past decade has witnessed a surge in the deployment of highly mobile CPS, such as autonomous ground vehicles and aerial drone swarms, for both civilian and military purposes. However, most existing systems remain centralized, dependent on a single control entity that dictates movement and coordination. This centralization introduces critical reliability concerns, especially in environments with unreliable communication or active interference (e.g., jamming).

My research aims to develop decentralized, fault-tolerant, and scalable swarming protocols that can maintain coordination even in the absence of centralized control. I plan to integrate ideas from fault-tolerant distributed computing with computational geometry to reason about coordination in dynamic, moving networks. While such problems are often NP-hard, I intend to exploit geometric structures such as Voronoi diagrams to design heuristic yet provably effective algorithms that perform well in practice.

In the future, I plan to unify these research directions to enable privacy-preserving and reliable autonomous CPS for use in adversarial environments. As hardware and energy storage systems like batteries evolve, mobile platforms like drones can carry lightweight GPUs and facilitate computationally intensive protocols like MPC. My ongoing work on lightweight cryptography and efficient MPC directly complements this evolution, enabling the design of secure, efficient, and resilient distributed intelligence for next-generation autonomous systems.

References

[1] Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, and Michael Reiter. Random Beacons in Monte Carlo: Efficient Asynchronous Random Beacons without Threshold Cryptographic Setup. In Proceedings of 31st ACM Conference on Computer and Communications Security (CCS), November 2024.

[2] Akhil Bandarupalli, Xiaoyu Ji, Aniket Kate, Chen-Da Liu-Zhang, Daniel Pöllmann, and Yifan Song. Computationally and Communication-Efficient Fair Asynchronous MPC: Scalable and Practical. *To Appear at* the 32nd ACM Conference on Computer and Communications Security (CCS), October 2025.

[3] Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, Chen-Da Liu-Zhang, and Michael Reiter. Delphi: Asynchronous Approximate Agreement for Financial Price Oracles and Drone Swarms. In Proceedings of 54th IEEE/IFIP Conference on Dependable Systems and Networks (DSN), June 2024.

[4] Akhil Bandarupalli, Adithya Bhat, Somali Chaterji, Michael K. Reiter, Aniket Kate, and Saurabh Bagchi. SensorBFT: Fault-Tolerant Target Localization Using Voronoi Diagrams and Approximate Agreement. In Proceedings of 44th IEEE International Conference on Distributed Computing Systems (ICDCS), July 2024.

[5] Choudhury, Ashish, and Arpita Patra. "An efficient framework for unconditionally secure multiparty computation." IEEE Transactions on Information Theory.

[6] Su, Yuan, Yuan Lu, Jiliang Li, Yuyi Wang, Chengyi Dong, and Qiang Tang. "Dumbo-MPC: Efficient Fully Asynchronous MPC with Optimal Resilience." In Proceedings of the 2025 USENIX Security Conference.

[7] Lu, Donghang, Thomas Yurek, Samarth Kulshreshtha, Rahul Govind, Aniket Kate, and Andrew Miller. "Honeybadgermpc and asynchromix: Practical asynchronous mpc and its application to anonymous communication." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.

[8] Abraham, Ittai, Yonatan Amit, and Danny Dolev. Optimal resilience asynchronous approximate agreement. In Proceedings of International Conference on Principles of Distributed Systems (OPODIS) 2004.

[9] Duan, Sisi, Xin Wang, and Haibin Zhang. Fin: Practical signature-free asynchronous common subset in constant time. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS) 2023.