



The Theory Group at the University of Michigan conducts research across many areas of theoretical computer science, such as combinatorial optimization, data structures, cryptography, quantum computation, parallel and distributed computation, algorithmic game theory, graph theory, geometry, combinatorics, and energy efficiency. We investigate the value of tradeoffs among fundamental resources such as running time, storage space, randomness, communication, and energy, in both the classical and quantum senses.

Theory faculty and students work with others from the division, as well as faculty from Mathematics, Electrical and Computer Engineering, Industrial and Operations Engineering, Climate and Space Sciences and Engineering, and elsewhere in the University.

## DESIGN AND ANALYSIS OF ALGORITHMS

**Faculty:** Seth Pettie, Quentin Stout, Grant Schoenebeck, Kevin Compton, Yaoyun Shi

Modern applications of computer science ultimately depend on having highly efficient algorithms for solving basic computational tasks; some examples are searching and summarizing a large corpus of textual data, finding optimal routes in networks, or finding an optimal solution to a set of linear inequalities. Efficiency is a fine goal, but what is it exactly? We try to characterize, in a mathematically rigorous way, the computational resources (running time, storage space, communication, energy, etc.) required to solve various combinatorial and optimization problems. We also investigate how changing the model of computation affects the complexity of solving specific problems. For example, we now know that quantum computers could solve some problems exponentially faster than a classical computer and that many other, but not all, problems can be solved significantly faster on a parallel computer.

Algorithms research at Michigan spans across many areas, including network optimization, approximation algorithms, the design and analysis of data structures, combinatorial problems in geometry, analysis of social networks, and algorithms for various parallel, distributed, and streaming models of computation.

## QUANTUM INFORMATION PROCESSING

**Faculty:** Yaoyun Shi, Igor Markov

Our goal is to sharpen the boundaries between the classical and the quantum worlds with respect to information processing. We investigate the following questions within the mathematical framework of quantum information science:

- For which kind of computational tasks can quantum computers dramatically outperform classical computers?
- To what degree can classical physics simulate and approximate quantum physics?
- How can one leverage quantum information to achieve higher efficiency and better security in communication?



## SECURE CRYPTOGRAPHIC PROTOCOLS

Faculty: Kevin Compton, Christopher Peikert, Yaoyun Shi

Cryptography is essential to electronic financial transactions and private communication so it is imperative that our cryptographic systems be truly secure against a variety of attacks. Below are two ongoing projects to (dis)prove the security cryptographic systems.

The first project deals with side channel attacks on cryptosystems. Small computing devices, such as smart cards, leak information through voltage fluctuations, radiation and other channels other than the standard input and output channels. It turns out that in some cases this side channel information reveals keys and other types of information stored on the smart card. The group is currently looking at different attacks and measures to protect against them.

The second project deals with cryptographic protocol security. When you buy something over the internet or log onto a remote site, you use various protocols where encrypted and secured information is sent over an open channel. Are these protocols secure? We are looking at different models of security and investigating new ways to automate the process of proving a protocol secure.

Yet another set of challenges are posed by quantum information technologies: how can we ensure that classical cryptographic protocols are secure against quantum adversaries, and how can we make use of quantum information to achieve unconditional security? We have developed methods for generating and distributing random numbers securely against all-powerful quantum adversaries, and are exploring many frontiers in quantum cryptography and post-quantum classical cryptography.

## PARALLEL AND DISTRIBUTED COMPUTATION

Faculty: Quentin Stout, Seth Pettie

For decades, the speed of processors was growing exponentially, but this has abruptly stopped. Instead, now the number of processor cores on a chip is growing exponentially. A graphics processing unit (GPU) in a laptop may have 100 cores, and supercomputers may have 1,000,000. At Michigan, we are developing algorithms and data structures that use parallelism to help solve large problems such as climate modeling and the design of ethical clinical trials.

Abstract models of parallelism are also investigated, such as having a large number of small entities (cores on a chip, smart dust, ants, robots) working together on the same problem. Algorithms may need to take physical location into account, where communicating with entities far away takes more time and energy. We also study abstract models of distributed computation, where a large number of independent, unsynchronized computers are arranged in a (possibly unknown) network and must solve a problem only through local communication.

## COMPLEXITY THEORY

Faculty: Grant Schoenebeck, Yaoyun Shi

Some computational tasks seem resilient to efficient solutions or even efficient approximation. When can we show that no efficient algorithm exists? What types of inputs are particularly difficult and why? What are the limits of quantum computing and parallelism? Besides the mathematical beauty of these questions, they have important applications to cryptography.

## THE INTERSECTION OF COMPUTER SCIENCE AND ECONOMICS

Faculty: Grant Schoenebeck, Satinder Singh Baveja, Michael Wellman

In today's online environments, computational agents engage with each other in commerce and other economically important activities. In such environments, agents must not reason only about their own actions, but also the actions of other agents. How can we design strategic agents that perform in dynamic and uncertain environments? Additionally, markets are being designed to allocate goods such as CPU time or advertising slots. How can we design new markets with desirable properties such as allocating goods to agents that most desire them? Market design can be thought of as an optimization problem where the inputs need to be elicited.

There are deep applications to social networks which can be viewed as a distributed system where each node operates in a local, autonomous, and, possibly, self-interested way. How can we reason about processes over such networks and what goals can be accomplished by such a network?



## FACULTY IN THEORY OF COMPUTATION



**Kevin Compton**  
Associate Professor  
kjc  
3603 Beyster Bldg



**Christopher Peikert**  
Patrick C. Fischer  
Development Professor of  
Theoretical  
Computer Science  
cpeikert  
3601 Beyster Bldg



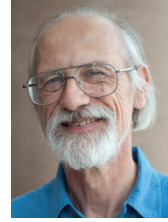
**Seth Pettie**  
Associate Professor  
pettie  
3628 Beyster Bldg



**Grant Schoenebeck**  
Assistant Professor  
schoeneb  
3636 Beyster Bldg



**Yaoyun Shi**  
Associate Professor  
shiyy  
3632 Beyster Bldg



**Quentin Stout**  
Professor  
qstout  
3605 Beyster Bldg

## AFFILIATED FACULTY

**Satinder Singh Baveja** - Computer Science and Engineering,  
Artificial Intelligence

**Andreas Blass** - Mathematics

**Parag Deotare** - Electrical and Computer Engineering

**Anna Gilbert** - Mathematics

**John Hayes** - Computer Science and Engineering, Hardware

**Mackillo Kira** - Electrical and Computer Engineering

**Jeffrey Lagarias** - Mathematics

**Igor Markov** - Computer Science and Engineering,  
Computer Architecture

**Viswanath Nagarajan** - Industrial & Operations Engineering

**Martin Strauss** - Mathematics

**Ilya Volkovich** - Computer Science and Engineering

**Michael Wellman** - Computer Science and Engineering,  
Artificial Intelligence

