Committee for the Advancement of Theoretical Computer Science CATCS

Richard Ladner

SIGACT Chair

Goals of CATCS

- Established in 2005 by SIGACT
- Promote theoretical computer science
  - Within CS, science and engineering community, the public
- Increase the funding levels for TCS
  - Foundations of algorithms
  - Applications of TCS in other initiatives
- Advocate for TCS
  - Funding agencies

Current Members

- Sanjeev Arora (Princeton), Chair
- Richard Ladner (University of Washington), ex officio
- Lenore Blum (CMU)
- Cynthia Dwork (Microsoft)
- Richard Karp (Berkeley)
- Richard Lipton (Georgia Tech)
- Michael Mitzenmacher (Harvard)
- Christos Papadimitriou (Berkeley)
- William Steiger (Rutgers),
- Salil Vadhan (Harvard)
- Avi Wigderson (Institute for Advance Study, Princeton)

Activities

- Workshops
  - Theory of Networked Computing, 2 (NSF funded)
  - Algorithms as a Lens on Science, 2 (NSF funded)
  - Visions for Theoretical Computer Science (CCC funded)
- Theory Matters wiki and mailing list
- Brochure
- Wikipedia Project
- Bi-weekly teleconferences
  - Close coordination with SIGACT
  - Guests such as CISE CCF director and program manager and DARPA program manager

Visions for TCS

- Held at University of Washington the day before STOC 2008, May 17, 2009
- Funded by Computing Community Consortium (CCC).
- Organizers: Bernard Chazelle, Anna Karlin, Richard Ladner, Dick Lipton, Salil Vadhan
- 32 Participants

Goals

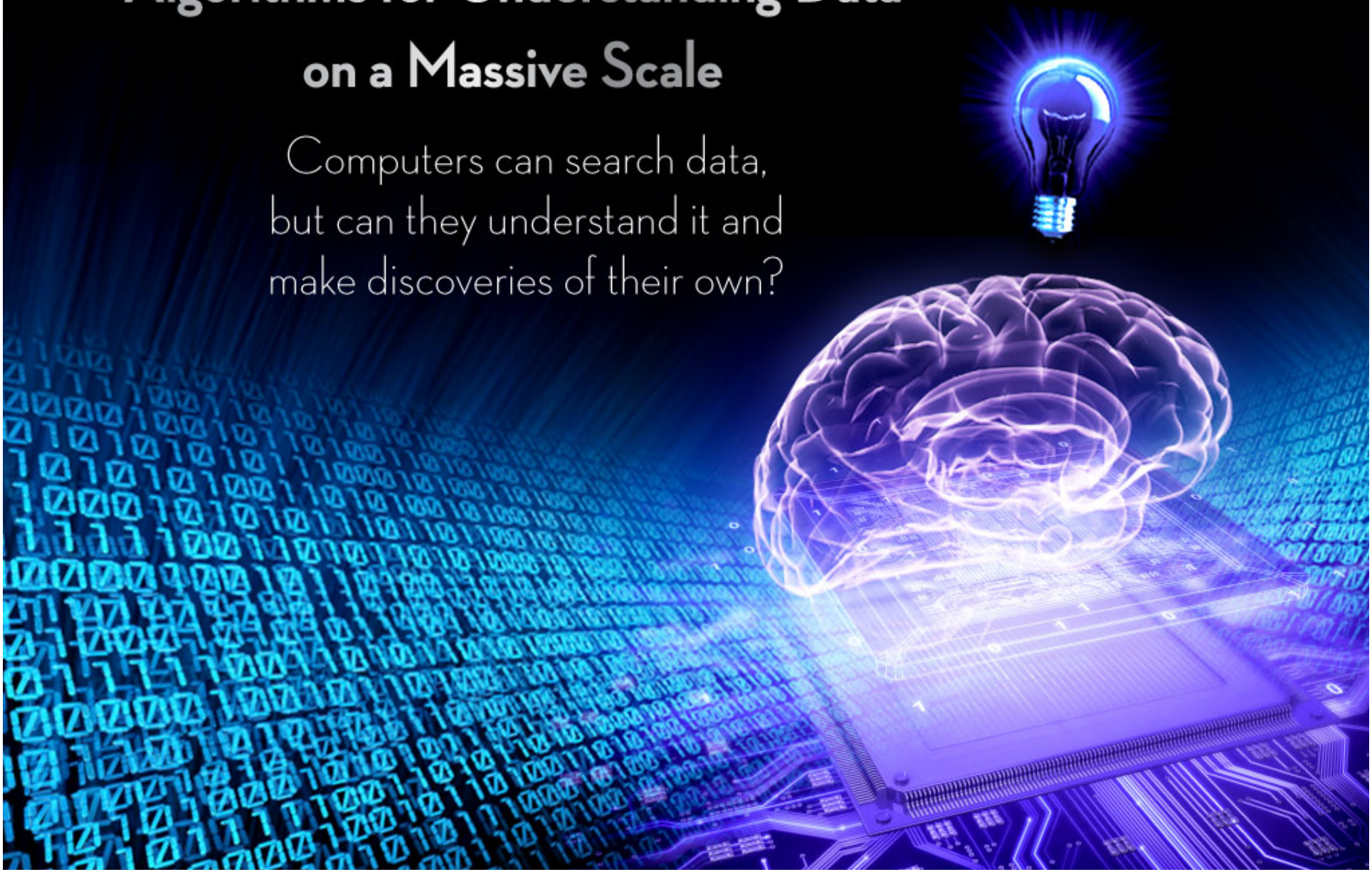
- Identify broad research themes within theoretical computer science (TCS) that have potential for a major impact in the future
- Distill these research directions into compelling nuggets that can quickly convey their importance to a layperson.
- Help CCC & others argue for the importance of fundamental (T)CS research to non-specialist audiences.

Nuggets

- Title
- Tag line
- Summary
- Rationale
- Image

Algorithms for Understanding Data on a Massive Scale

Computers can search data, but can they understand it and make discoveries of their own?



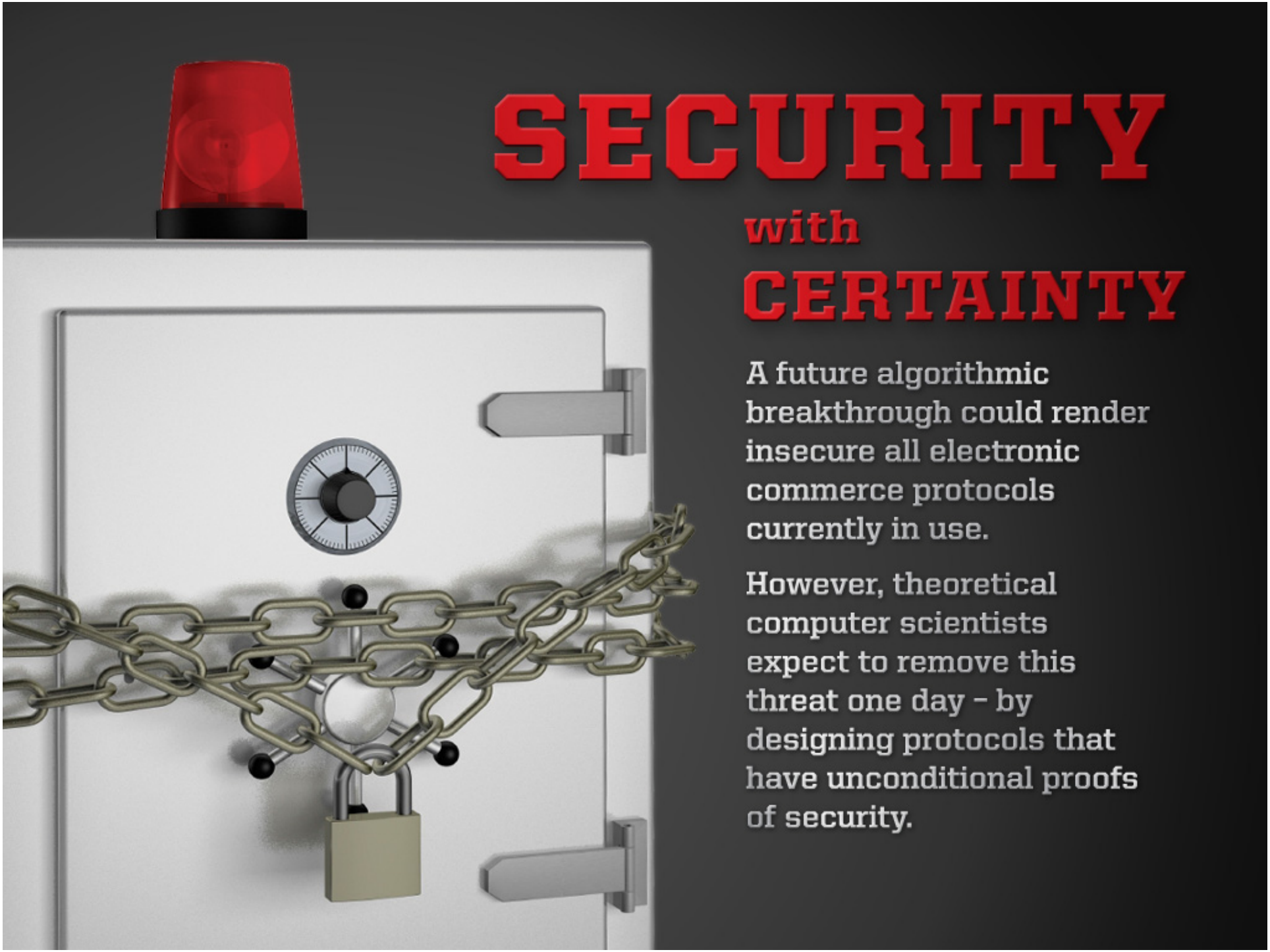
Algorithms for understanding data on a massive scale

Tag Line

Computers can search data, but can they understand it and make discoveries of their own?

Summary

During the last decade we have witnessed a dramatic increase in the amount of generated data. The web, network traffic, scientific, health, financial and marketing data sets are a few examples of the massive and heterogeneous data being produced in unprecedented volume. The data often contains information of great value. For example, computers could cross-examine genetic and clinical health data in order to design cures for diseases. However, extracting knowledge from terabytes of raw data requires extremely efficient algorithms, posing a great challenge to algorithm designers.


SECURITY
with
CERTAINTY
A future algorithmic breakthrough could render insecure all electronic commerce protocols currently in use.
However, theoretical computer scientists expect to remove this threat one day – by designing protocols that have unconditional proofs of security.

Security with Certainty

Tag Line

A future algorithmic breakthrough could render insecure all electronic commerce protocols currently in use. However, theoretical computer scientists expect to remove this threat one day --- by designing protocols that have unconditional proofs of security.

Summary

Modern research in cryptography has transformed a significant portion of computer security from an art into a science. Instead of merely hoping that a clever adversary will not find a way to break the system, we can now *prove* the security of cryptographic protocols (encryption, digital signatures, etc.) on precise computational conjectures. For example, we can construct algorithms for encrypting messages so that it is computationally infeasible for anyone other than the intended recipient to learn anything about the message from its encryption, *under the assumption* that there are no fast algorithms for factoring large integers. Can security of this type be achieved *under no assumptions?*

Other Nuggets

- Nearly Completed
  - Communication Complexity
  - The Computational Lens on Economics
  - Efficient Computation in the Physical Universe
  - Modeling and Exploiting the Power and Parallelism of Tomorrow's Computers
- In progress
  - The Best of Both Worlds: Achieving Privacy and Utility
  - Computational Approaches to Modeling the Brain and the Cell
  - Computational Properties of Prediction Markets
  - Computing as a Commodity: Distributed Computing over the Global Internet
  - Economics and the Internet
  - Life-Critical System Verification
  - Making Economic Theory Tractable
  - P $\neq$ NP as a Law of Nature

Theory Matters Wiki

- Open Wiki that allows collaboration and information flow within the theory community
  - www.theorymatters.org
- Nuggets
- Various white papers on importance and directions in theory
- Funding resources