SIMONS INSTITUTE for the Theory of Computing

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

The New DIMACS/Simons Collaboration in Cryptography

[June, 2015] DIMACS announces an upcoming Special Focus on Cryptography as part of a broader partnership with the Simons Institute for the Theory of Computing. The new DIMACS/Simons Collaboration in Cryptography features activities at both DIMACS and the Simons Institute, bringing together cryptographers and others to advance the state of the art in cryptography toward systems that are simultaneously highly efficient, highly secure, and highly functional. About the new venture, DIMACS Director Rebecca Wright says, "We are pleased to be partnering with the Simons Institute on this exciting topic. Cryptography requires both theoretical and practical advances, and we believe our joint program will contribute to dramatic progress in the field."

Cryptography is one of the most important tools in securing data, communication, and cyberinfrastructure. Driven by ever-increasing amounts of data and the associated computational demands, organizations and individuals are outsourcing storage and computation to "the cloud." As our e-mail, medical, financial, and other personal information increasingly reside in systems outside of our direct control and are of increasing value to attackers, the need to simultaneously guarantee privacy, availability of data, and correctness of computations is paramount. This digital reality poses complex challenges to cryptography and requires a paradigm shift in our goals and mode of thinking. Overarching goals of the collaboration include expanding our understanding of such things as: how to verify the correctness of outsourced computations; what primitives and performance can be obtained from specific intractability assumptions; how to provide selective access to parts of encrypted data; the implications of fundamental tradeoffs and impossibility results; and how best to drive adoption by system designers and implementers of more secure technologies and practices. By studying these and other questions, the collaboration seeks to enable foundational theoretical advances in cryptography together with practical advances in its usability.

The DIMACS/Simons Collaboration kicks off with an intensive Program in Cryptography underway at the Simons Institute during the summer of 2015, and it continues with the two-year Special Focus on Cryptography at DIMACS scheduled to start in late 2015. Beginning with a Cryptography Boot Camp to introduce key themes, the Simons program brings together over 90 long-term participants with a strong focus on the foundations of cryptography and related new mathematical questions. The Simons program also includes workshops on Securing Computation and on the Mathematics of Modern Cryptography.

The DIMACS Special Focus builds on the Simons program to involve a broader range of people, bringing cryptographers together with other security researchers, programming language researchers, and software engineers. It aims to advance the state of the art and practice of

cryptography via research visits, sponsorship of NYCryptoDay, and seven additional workshops that are currently being planned on the topics of:

- Cryptography for Big Data
- Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures
- Cryptography for the RAM Model of Computation
- Advances and Limits of Program Obfuscation
- Efficient and Usable Secure Computation
- Complexity of Cryptographic Primitives and Assumptions
- Outsourcing Computation Securely

Both DIMACS and the Simons Institute coordinate many of their activities around designated scientific themes (like cryptography). While themed programs at the Simons Institute typically span a single semester, DIMACS special foci typically span several years. The Collaboration in Cryptography aims to leverage these different timescales. The intense focus and energy of the Simons program will launch the collaboration and build momentum around the cryptography theme, while the longer time afforded by the DIMACS special focus will allow ideas to broaden and develop more fully. Simons Institute Director Richard Karp says, "This exciting partnership will engage a broad community of researchers and practitioners, and promises to spur progress in both the theory and the practice of cryptography."

The Collaboration in Cryptography is the first between the two centers, and both Karp and Wright hope that it will be a model for future such collaborations. In addition to DIMACS and the Simons Institute, the Collaboration in Cryptography is working with the Center for Encrypted Functionalities at UCLA, the Modular Approach to Cloud Security project at Boston University, and the Data Science Institute at Columbia University on individual workshops to be held as part of the DIMACS special focus.

The DIMACS/Simons Collaboration in Cryptography is funded by the National Science Foundation as a research coordination network under award CNS-1523467. The Simons Institute program is supported in part by a grant from the Simons Foundation.

Related Links:

- Special Focus on Cryptography: http://dimacs.rutgers.edu/SpecialYears/2015_Crypto/
- DIMACS/Simons Collaboration in Cryptography: http://dimacs.rutgers.edu/DIMACS-SimonsCrypto/
- Simons Institute for the Theory of Computing: http://simons.berkeley.edu/
- Simons Institute Program in Cryptography: http://simons.berkeley.edu/programs/crypto2015
- NYCryptoDay: https://nycryptoday.wordpress.com /