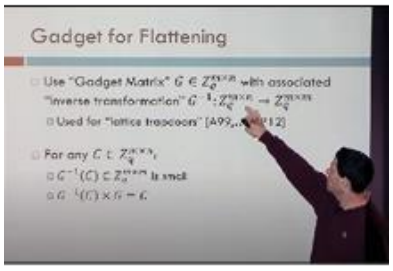
DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

Reflecting on the DIMACS/Simons Collaboration in Cryptography

[July, 2020] Earlier this year, the DIMACS Special Focus on Cryptography said goodbye to its final visitor to conclude both the special focus and the larger DIMACS/Simons Collaboration in Cryptography that contained it. Funded by the National Science Foundation (NSF) as a research coordination network (RCN), the DIMACS/Simons Collaboration was the first formal partnership between DIMACS and the Simons Institute for the Theory of Computing.

The Collaboration in Cryptography was devoted to advancing important goals in cryptography research through activities held at both DIMACS and the Simons Institute. These goals included understanding: what primitives and performance can be obtained from specific intractability assumptions; where there are fundamental tradeoffs or impossibility results; and how best to drive adoption by system designers and implementers of more secure technologies and practices. Toward these goals, project activities brought cryptographers together with mathematicians, security researchers, programming language researchers, and software engineers to advance both the foundations and applications of cryptography through workshops and research visits.



From top: Logo for the Simons Institute Cryptography Program; Shai Halevi presenting at the Simons Institute; Muthu Venkitasubramaniam presenting at DIMACS; Panel at Advanced Crypto Standardization.

The Collaboration in Cryptography began with an intensive program on cryptography at the Simons Institute during the summer in 2015, and it continued with a multi-year Special Focus on Cryptography at DIMACS. The Simons program involved 96 long-term visitors to the Simons Institute, nearly half of whom received some form of support from the RCN project. Having such a large group of researchers in cryptography theory together at the Simons Institute facilitated collaboration, leading to remarkable productivity and a flood of subsequent publications. The Simons program also featured many community-building activities, such as reading groups, a seminar series featuring historical papers, and mentoring lunches for students and postdocs.

The DIMACS special focus began in the fall of 2015 to sustain collaborations begun during the Simons program and expand them to include more people and more topics. The Special Focus on Cryptography sponsored 10 events that involved roughly 900 participants, and it hosted 11 visitors. The special focus events were:

1) DIMACS/Columbia Data Science Institute Workshop on Cryptography for Big Data
2) DIMACS/MACS Workshop on Cryptography for the RAM Model of Computation
3) DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures
4) DIMACS/CEF Workshop on Cryptography and Software Obfuscation
5) DIMACS Workshop on Complexity of Cryptographic Primitives and Assumptions
6) DIMACS Workshop on Outsourcing Computation Securely
7) Beyond Crypto: A TCS Perspective (affiliated with Crypto 2018)
8) DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation
9) Reconnect 2019: Cryptography
10) Workshop on Advanced Cryptography Standardization (affiliated with Crypto 2019)

In the spirit of research coordination, events of the DIMACS special focus reflect coordination with the Columbia Data Science Institute, two SaTC frontier projects—the Center for Encrypted Functionalities led by UCLA and the Modular Approach to Cloud Security project led by Boston University—and association with the Crypto Conference in 2018 and 2019, which began holding affiliated events in 2018. The special focus was also a sponsor of NYCryptoDay, a long-running series of one-day events held at rotating locations around the greater NYC area. CryptoDay strengthens ties within the local cryptography community while showcasing the latest research in cryptography.

Participants in RCN activities conducted at both the Simons Institute and DIMACS reported a trove of new results that now appear in over 150 papers. These results include foundational advances in the study of interactive proofs for verifying the correctness of computations delegated to the cloud; progress in understanding the round-complexity of non-malleable cryptography to efficiently enable strong security guarantees in distributed settings; breakthroughs in constructing efficient secure multi-party computation protocols under discrete-log assumptions to break the so-called circuit-size barrier; a foundational study on the bitcoin protocol; and exciting progress on simplifying and weakening the objects and assumptions that imply indistinguishability obfuscation (IO), deepening understanding of this fundamental object, and taking large strides toward the goal of basing the existence of IO on well-studied assumptions. Many of these results enable simpler, more efficient, and ultimately, more practical cryptographic systems. The project also helped to promote standardization efforts that will help to move advanced cryptographic technologies closer to practical use.

The idea for the DIMACS/Simons Collaboration in Cryptography was sparked by discussions between former DIMACS Director Rebecca Wright and former Simons Institute Director Richard Karp at a meeting of the DIMACS Advisory Board on which Karp served. As Wright recalls, “It quickly became clear that the short, intensive programs of the Simons Institute would blend well with the longer length and sustained energy of a DIMACS special focus. The two institutions complement each other in a combined program, and this realization led us to the general model for the Collaboration in Cryptography.”

It was such a good model that the Collaboration in Cryptography became the model for two subsequent DIMACS/Simons Collaborations in Bridging Continuous and Discrete Optimization and in Lower Bounds in Computational Complexity, both of which are ongoing. David Pennock, who took the reins as director of DIMACS in January, hopes for more. He says, “I love this idea of research coordination. It’s exactly what we do at DIMACS. The collaborations with the Simons Institute have worked well and the RCN model is one that I hope to replicate and build on in the future.”

Related Links:

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