WAM 2018 Yearbook
Mathematics of Modern Cryptography

Institute for Advanced Study, Princeton
May 19-25, 2018

This is a compilation of activities and resources contributed by participants during the 2018 Women and Mathematics Program. We hope this can serve as a mathematical and professional reference guide for women mathematicians around the country.

I. Mathematical Talks

A. Terng Lectures:

Toni Bluher, National Security Agency, "Mathematics in Cryptography"

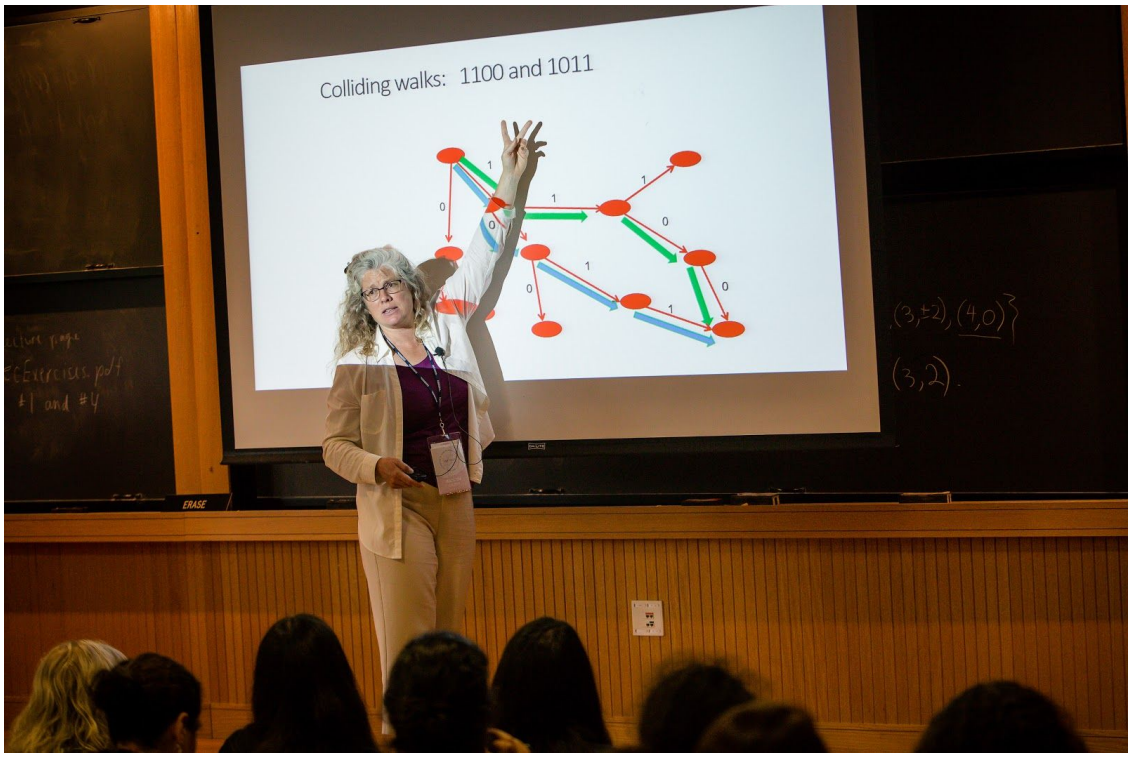
Abstract: This introductory course aims to convey the evolutionary nature of cryptography and the central role of mathematics in this story. Topics include substitution ciphers and how to defeat them, WWII cryptography, symmetric cryptography and electronic codebooks, authentication, public key cryptography, mathematical underpinnings of internet security, and the future.

- Lecture 1: Enigma
  - Video
  - Rejewski paper
  - Slides
- Lecture 2: Public Key Cryptography
  - Video
  - Slides
  - Protocols
  - Background on Elliptic Curve Arithmetic
  - Exercises

- Lecture 3: Public Key on the Internet
    - Video
    - Slides
- Lecture 4: The Future.
    - Video
    - Slides
- Mini Lecture: Video Cash (Emily Willson)
    - Slides

B. Uhlenbeck Lectures:

Kristin Lauter, Microsoft, "Mathematics in Post-Quantum Cryptography"



Abstract: This course will cover some of the mathematics behind current proposals for Post-Quantum Cryptography (PQC). In 2017, the National Institute of Standards and Technology launched a multi-year international competition to select new post-quantum cryptographic systems, based on hard problems in mathematics for which there are no known polynomial time quantum algorithms. These lectures will cover some of the mathematics of lattice-based cryptography, code-based cryptography, homomorphic encryption, and Supersingular Isogeny Graphs, and will highlight some of the deep connections with number theory.

- Lecture 1: How to Keep your Secrets in a Quantum World
  - Video
  - Slides
  - Exercises
- Lecture 2: Hardness of Supersingular Isogeny Graph-based Cryptography

    - Video
    - Slides
    - Exercises
- Lecture 3: Theory and Practice of Homomorphic Encryption
    - Video
    - Slides
    - Exercises
- Lecture 4: Security Considerations for LWE/RLWE
    - Video
    - Slides

References

Jeff Hoffstein, Jill Pipher, Joseph H. Silverman, An Introduction to Mathematical Cryptography, Undergraduate Texts in Mathematics, Springer, 2008.

Richard A. Mollin, An Introduction to Cryptography, Chapman & Hall/CRC, 2001.

Richard A. Mollin, RSA and Public-key Cryptography, Chapman & Hall/CRC, 2003.

Wade Trappe and Lawrence C. Washington, Introduction to Cryptography with Coding Theory, 2002. Second edition (2006)

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, 2nd edition (or more recent if available), Chapman & Hall/CRC, 2003. Second edition (2008)

Joseph H. Silverman and John Tate, Rational Points on Elliptic Curves, New York: Springer Verlag, (1955).

Joseph H. Silverman, The Arithmetic of Elliptic Curves, New York: Springer Verlag, (1955).

C. Colloquium

Jill Pipher, Brown University, "NTRU Lattice-based Algorithms: History and Modern Developments"

Abstract: This lecture will contain some historical information about the development of lattice-based algorithms in cryptography, with a special focus on NTRU. Modern developments related to homomorphic encryption and quantum computing will be discussed.

Video

D. Research Seminar

Organized by Fattaneh Bayatbabolghani and Betül Durak

- Kelsey Horan, "A Fast Quantum Algorithm for Solving Multivariate Quadratic Questions"
- Angela Robinson, "The Tractability of the Discrete Logarithm Problem in S_n and Hybrid Encryption in the Quantum Random Oracle Model"
- Elizabeth Wilcox, "The Chermak-Delgado Lattice of a Finite Group"
- Ha Tran, "Well-known Ideal Lattices from Cyclotomic Fields"
- Fattaneh Bayatbabolghani, "Enforcing Input Correctness via Certification in Gabled Circuit Evaluation"
- Betül Durak, "Breaking the Format-Preserving Encryption Standard Over Small Domains"
- Soodeh Dadras, "Security of Control Systems in Autonomous Vehicle Platooning"


2019

E. Princeton University Day Activities

Talks by:

- Oanh Nguyen, Instructor of Mathematics, Princeton University, "The mixing time of the Diaconis-Gangolli random walk on contingency tables over $\mathbb{Z}/m\,\mathbb{Z}$"
- Ana Menezes, Assistant Professor of Mathematics, Princeton University, "Minimal surfaces in homogeneous spaces"
- Yueh-Ju Lin, Instructor of Mathematics, Princeton University, "Conformal geometry and partial differential equations"

Computer Workshop:

- Instructor: Alyson Deines, Center for Communications Research
- TA: Linda Cook, Graduate Student, Applied & Computational Mathematics, Princeton University

II. Women in Science Seminars

A. Work/Life Balance panel, moderated by Lillian Pierce (Duke).
Panel: Toni Bluher (NSA), Dusa McDuff (Columbia), Margaret Readdy (U Kentucky), Christelle Vincent (U Vermont).

B. After dinner chat with Jill Pipher (Brown).

C. Career panel, moderated by Jessica Fintzen (IAS).
Panel: Toni Bluher (NSA), Kristin Lauter (Microsoft), Helen Wong (IAS), Helen Xing (Cubist).

D. Intersectionality in Mathematics, moderated by Yen Duong and self-organized by WAM participants.
This informal working lunch group first listed different aspects that make up our identity (gender, race are the easy ones, but then disability, socioeconomic class, geographic roots... It was a long list). Broke into small groups and discussed how these aspects affect our lives as mathematicians, how to balance them, how they affect our views of success, and wrapped up with a ten minute writing exercise exploring our values.

E. Resources:

History of Cryptography:

- Marion Rejewski, An applicaiton of the theory of permutations in the Enigma Cipher
- DeBross & Burke, The secret in Building 26. Defeating the German Enigma
- Center for Cryptologic History
- David Kahn, Codebreakers
- David Kahn, Code Girls
- Imitation game (movie)

Sage:

- Can download source code github.com/sagemath
- Sage Wiki
- LMFDB -- online database of elliptic curves

Negotiating your work conditions:

- Individual salary data is public information for public universities. Google individual universities or see the Public University salary database
- Ask for research travel monies (for you and your collaborators), laptop, software, relevant journal subscriptions in start-up package.
- Many universities provide modified leave after birth/adoption of child for one or both parents.
- Pause the tenure clock for life events.
- Do not be afraid to ask! Often you will be the first person ever in your department to realize there is room for improvement in a particular area. Doing so will make the environment of your department more attractive to future faculty hires.

Choosing your advisor:

- Take classes and attend seminars to meet faculty.
- Ask advanced graduate students about their advisors.

Intersectionality and Overlapping Identities:

- On the Intersecting Nature of Privileges and Oppression by Nicki Lisa Cole
- See page 6 of WAM 2016 Yearbook.

Further resources:

- The AWM website has a vast trove of resources, including information on travel grants, research conferences, student chapters and AWM workshops.
- Nebraska Conference for Undergraduate Women in Math Registration opens in early October -- apply early.
- Sascha Grau's on-line elliptic curve visualizer
- The 2016 WAM Yearbook has resources on careers in math, GRE advice, travel grants, gender issues in STEM, starting on page 7.
- The 2017 WAM Yearbook has resources for organizing an Ambassador program activity and work/life balance.
- The IAS School of Mathematics has a Summer Collaborators program. Application due date is usually December 1st.

III. Outreach

A. "Secrets and Codes" outreach at Littlebrook Elementary School.
Organized by Margaret Readdy with help from M^3 = Quiyana Murphy, Kayla Mesh and Miranda Moore.

B. Introduction to Ambassador Program

Thanks to a generous grant from Lisa Simonyi, the IAS Women and Mathematics Program will fund annually up to three (3) postdoctoral or advanced graduate ambassadors and up to six (6) graduate ambassadors to build support and outreach networks across the country.

WAM Ambassador selection criteria include previous participation in the Women and Mathematics summer program, mathematical expertise, and enthusiasm. Each lead conference organizer and graduate ambassador should have a faculty sponsor (male or female) at their home institution.

WAM Ambassadors must also fulfill these requirements:

1. Submit a summary report within 30 days of the completion of the proposed activity.
2. Acknowledge IAS Women and Mathematics and Lisa Simonyi in activity announcements (print and online) and in any publication that results from the activity.
3. Participate in the WAM annual meeting the following May to share best practices and new outreach ideas, and to help train new WAM Ambassadors.

See www.math.ias.edu for details.

C. Ambassador Program Reports

The WAM participants listened to one representative from each of the funded groups and were able to ask questions regarding organizing similar activities in their own region.

The funded activities were:

1. A series of 15 research talks, panels, workshops and social events for the UC Santa Barbara AWM student chapter.
2. Carolinas Women in Mathematics Symposia.
3. University of Michigan Women in Mathematics (WIM) and AWM events, including graduate school panel and linear algebra study nights.

4. Gender equity in mathematical studies (GEMS) group at UC Berkeley. Activities included a reading group, outreach at a local middle school, GRE preparation sessions.
5. Women and Mathematics at Carnegie Mellon (WAM@CMU) conference.
6. "Arithmetic of algebraic curves" conference at the University of Wisconsin.
7. Brown University Horizons Reading Group focusing on the social implications of big data.
8. Harvard/MIT Graduate Workshop in Algebraic Geometry for Women and Mathematicians of Minority Genders https://sites.google.com/view/gwag.

III. WAM 25th Anniversary Celebration!

The Women in Mathematics Program honored individuals who have been involved with founding WAM and establishing it at the Institute, from its inception at MSRI to IAS/Park City to its present-day location at the Institute for Advanced Study.

Antonella Grassi, Chuu-Liang Terng and Karen Uhlenbeck were among the many honorees. The event is featured in the July--August 2018 AWM Newsletter. Karen Uhlenbeck's banquet speech appears on pages 21 and 22 of the newsletter.

WAM 2018

Links to stay in touch:

IAS WAM 2018 Facebook page

2018 Program

WAM website

IAS