Applied Mathematics for Secure and Trustworthy Cyberspace
SaTC 2019 PI meeting breakout group report

Co-leads: Steve Miller (Rutgers) and Vinod Vaikuntanathan (MIT)

1. Problem/Domain Summary

The topic of the group was “Applied Mathematics for Secure and Trustworthy Cyberspace”. Much if not all modern cryptography, and hence the foundations of a secure and trustworthy cyberspace, rests on the computational difficulty of mathematical problems. Especially in recent years in cryptography, we have increasingly relied on *new mathematics* for:

a. *Stronger Security*, including security against quantum computers (or “post-quantum cryptography”);
b. *Richer Functionality*, starting from public-key encryption in the 1970s, to identity-based encryption in the 1990s, to fully homomorphic encryption in the 2000s, and to the current frontier of program obfuscation in this decade; and
c. *Better Efficiency* under old and new metrics.

Cryptographers need to develop new cryptosystems using new mathematical problems (partly as insurance in case current cryptosystems are attacked and partly to advance the frontiers of what can be accomplished). To ensure solid foundations of these new cryptosystems, cryptographers, in collaboration with domain experts (i.e., mathematicians), need to better understand the mathematical and algorithmic properties of the newly proposed problems.

2. Key Research Challenges

Cryptography and SaTC needs the involvement of mathematicians. The key challenge is how to accomplish this in a productive, smooth, and efficient way. What is the best way for cryptographers to communicate the problems of interest (to other cryptographers and) to applied mathematicians? What should mathematicians work on, in order to maximize their usefulness (to SaTC)? How can cryptographers find more details about the mathematical context of a problem they are interested in, or the state of the art on it?

3. Potential Approaches

The breakout session was attended by 20-25 researchers (from math, crypto and security communities) over the two days. We discussed both specific and general approaches.

The specific approaches were to go over mathematical problems that are compelling and of recent interest in the field. Three presentations were made, by Amit Sahai (on solving systems of polynomial equations over the integers with applications to program obfuscation), Nadia Heninger (on possible backdoors in the Micali-Schnorr pseudorandom generator), and Dan Boneh (on class groups of imaginary quadratic number fields with applications to verifiable delay functions). The presentations were accompanied by robust discussion and input from many of the attendees.

The general approach was aimed at creating forums for more (productive) interaction between mathematicians and cryptographers/security researchers. We discussed the following avenues:

1. Creating a moderated blog/wiki and/or seeking to develop a separate section of the eprint archive as (a) a repository of open problems with short, precise and accessible descriptions where mathematicians and cryptographers could distribute their ideas to a targeted audience; and (b) a way to systematize knowledge in relevant mathematical fields important for cybersecurity researchers, enabling faster and easier access.

2. Polymath projects to make progress on important mathematical problems of cryptographic relevance were also discussed in relation to the general idea of online forums and collaboration.

3. Targeted workshops aiming to bring together the two communities. Recent examples include a Banff workshop, an AIM workshop, a recent ICERM workshop etc. Another example is Mathcrypt, a workshop co-located with the Crypto conference.

4. Survey articles, in the mold of Dan Boneh's highly praised survey "Twenty years of attacks on the RSA cryptosystem" published in the *Notices of the American Mathematical Society* in 1999.

4. Long-Term (> 10 years) Significance

Because of the fundamental importance of mathematics in cybersecurity, we expect the need for mathematicians and for stronger ties between the cryptography and pure/applied mathematics communities to grow stronger over the coming decades, even as more mathematicians are (hopefully) integrated into the SaTC community.

5. Other Important Aspects of This Topic *(specify)*

Even in this day and age where preprint servers have become more prominent, the status of publications was an important part of the discussion. For example, related to item 1, how to put in place mechanisms that incentivize participation in moderating/submitting to a blog/wiki? In relation to item 3, we also discussed the difference in publication venues in the two communities (conferences for cryptographers and journals for mathematicians). In relation to item 4, we discussed what could be appropriate venues for survey articles aimed to reach a broad spectrum of mathematicians (Notices of AMS is one possibility.)