Constructing cryptographic multilinear maps

organized by
Dan Boneh, Ted Chinburg, Alice Silverberg, and Akshay Venkatesh

Workshop Summary

Overview

The goal of the workshop was to bring together mathematicians and cryptographers to work on a major problem in cryptography and computer security, namely the problem of constructing secure and efficient cryptographic multilinear maps. Cryptographic multilinear maps are an extremely powerful tool in cryptography. They solve many long-standing open problems in the field that currently cannot be solved any other way (for example, code obfuscation and group key exchange). Unfortunately, all known constructions are extremely inefficient and have been shown to be insecure for some applications.

The Weil pairing on elliptic curves, or more generally abelian varieties, gives rise to efficient and secure 2-way cryptographic multilinear maps (known as cryptographic bilinear maps). The goal of this workshop is to construct an efficient and secure construction of n-way cryptographic multilinear maps when $n > 2$. The workshop gave a unique opportunity for a mix of cryptographers and mathematicians to work together to make progress on this open problem.

The workshop brought together a diverse group of scientists with a mixture of expertise from mathematics and computer science, and also from the cryptographic (building and constructing useful cryptographic objects) and cryptanalytic (attacking the security) sides. Such a mix is crucial to make sure that proposed solutions survive the tests of being both efficient and secure.

The format of the workshop was ideal for this topic, with a couple of talks each day, and most of the time devoted to working on interesting problems. The talks were designed to bring the participants up to speed on the topic, past attempts at constructions and related attacks, and possible avenues for future progress. It was important for this diverse group to develop a common language so we could communicate well on both the questions and possible solutions; the talks, the discussions at lunch and the breaks, and the working groups were all very important in achieving this.

At the workshop, the participants explored constructions from structures that arise in algebraic geometry, number theory, and topology, and considered a number of possible avenues for attack on the security of various cryptosystems.

Activities

Monday morning began with an extended overview of cryptographic multilinear maps by Dan Boneh. This was followed by a talk by Amit Sahai on indistinguishability obfuscation, which is a form of code obfuscation, and is a major application of cryptographic multilinear

maps. Monday afternoon consisted of a long Open Problems Session, moderated by Kristin Lauter. Many problems were suggested and discussed, leading to a nice choice of problems for Working Groups to form around for the remainder of the week.

On Tuesday morning, Rachel Lin gave a talk on how to achieve indistinguishability obfuscation from cryptographic multilinear maps. Then Mehdi Tibouchi gave a talk on multilinear map constructions. On Tuesday afternoon, the participants split up into three working groups (more on the working groups below). The interest in the problems, and the synergy of the groups, was so great that no one wanted to break for the reception.

Wednesday morning consisted of lectures presenting currently known attacks on multilinear map constructions; the talks were given by Mark Zhandry, Jung Hee Cheon, and Changmin Lee. The afternoon was devoted to the Working Groups.

On Thursday morning, Alice Silverberg gave a talk on the "impossibility result" in the 2003 Boneh-Silverberg paper (Corollaries 7.6 and 7.7 in that paper), two of the Working Groups gave reports on their progress thus far (with lively discussions by the full group), and Kristin Lauter gave a talk on Ring Learning With Errors (RLWE). Working Groups met in the afternoon.

Friday morning began with a report to the whole group, and general discussion, concerning the remaining working group. This was followed by a talk by Martin Bright on Brauer groups. People worked together in groups in the afternoon (including subsets and permutations of the earlier Working Groups), and the workshop ended with the entire group listening to reports from these groups, and discussing progress attained thus far and promising approaches for the future.

Working Groups

One of the Working Groups focused on elliptic curves. The primary thrust was to find a way to use supersingular elliptic curves to construct cryptographically secure 3-way (or n-way for any $n \geq 3$) multilinear maps, or achieve 4-way (or n-way for any $n \geq 4$) group key exchange. The classic Diffie-Hellman protocol enables two parties to communicate securely, by generating a shared secret key that is unknown to the adversary. If n parties want to communicate securely in one round, this is called n-way group key exchange. The three-party case was solved by Joux in 2000 using pairings on elliptic curves. Recently, supersingular elliptic curves have been used to perform 2-party key exchange that is currently believed to be resistant to quantum attack, due to the presumed difficulty of computing an (unknown) isogeny between two isogenous supersingular elliptic curves. Another direction the group looked into was to try to find cryptographic bilinear maps whose target is the group of points on an elliptic curve over a finite field. The working group generated concrete ideas on these questions, and we expect to see them written up for publication in the near future.

A second Working Group had the goal of using cohomological techniques coming from algebraic geometry to construct cryptographic multilinear maps. Several different cup product and Massey product constructions in étale cohomology were considered. A case studied in detail involved abelian surfaces over finite fields. Two different trilinear maps to roots of unity were considered. One required fixing an isogeny first, with the three groups in the map being torsion subgroups of the dual abelian variety. The other map did not require fixing an isogeny, but one of the groups involved is a torsion subgroup of the Brauer group of the surface. The computability and security of these candidates will be studied in the coming

months. A main conclusion of the workshop is this work will either lead to (i) a cryptographic multilinear map, or to (ii) significant new bounds, both from above and below, on the computational complexity of determining cup products in étale cohomology for varieties over finite fields.

A third Working Group worked on finding new attacks on existing cryptographic multilinear maps. This group considered, in particular, attacks on local pseudo-random number generators, and algorithms to solve approximate gcd problems for "general parameters". The group obtained experimental results on using Gröbner bases to break certain proposed local pseudo-random generators.