An Algebraic Approach to Multilinear Maps for Cryptography (18w5118)

Alice Silverberg (University of California, Irvine),
Dan Boneh (Stanford University)
Ted Chinburg (University of Pennsylvania)

May 6 – May 11, 2018

1 Objectives

A main goal of the BIRS workshop "An Algebraic Approach to Multilinear Maps for Cryptography" was to bring together cryptographers, number theorists and arithmetic geometers to discuss problems of central importance in electronic communication. The focus of the workshop was on cryptographic multilinear maps. It is an open problem to construct secure cryptographic multilinear maps with more than two arguments in their domain [1]. A solution to this problem would have many applications. These include allowing groups of people to share a common secret securely and the ability to obfuscate computer programs in order to protect the intellectual property they represent. The workshop also dealt with other problems in cryptography such as quantum computation, pseudo-random number generators and applications of isogenies of abelian varieties to cryptography.

Two specific objectives of the workshop were to

(i) analyze various proposed constructions of cryptographic multilinear maps, and

(ii) familiarize the participants with open problems in number theory and arithmetic geometry arising from cryptography.

The workshop brought together researchers and advanced Ph.D. students working on cryptography and related topics in number theory and arithmetic geometry.

The workshop was timely in view of recent research activity in this area. It built on progress resulting from an AIM workshop organized by the same organizers in October of 2017.

Besides the generous support from the Banff International Research Station, this workshop was also supported by an SaTC award from the National Science Foundation titled "An algebraic approach to secure multilinear maps for cryptography." The P.I.'s on this NSF SATC award were the organizers (Silverberg, Boneh and Chinburg) and A. Venkatesh.

The workshop had 29 participants and ten scheduled 50-minute talks. In between these talks, the participants broke into working groups to discuss particular questions arising from the talks as well as new ideas related to the subject of the workshop.

2 Talks

In the following we give a description of each talk, in the order in which the talks were given.

2.1 Alice Silverberg, Introduction to cryptographic multilinear maps.

The talk introduced the concept of a cryptographic multilinear map as in [1], starting from basic concepts familiar to the diverse audience of the workshop, who consisted of both mathematicians and computer scientists. In addition to presenting some open problems to be considered during the workshop, a goal was to give the participants a common language and background on which to build. The talk began with Diffie-Hellman key exchange [4], and went on to present the one-round tripartite Diffie-Hellman protocol of Joux [12], and an identity-based key agreement scheme of Sakai, Ohgishi, and Kasahara [17]. We also mentioned a destructive use of pairings due to Menezes, Okamoto, and Vanstone [14].

2.2 Dan Boneh: Background on multilinear maps, and applications.

The talk defined the notion of a cryptographic multilinear map and explored applications of such maps in cryptography. Applications include digital signatures, broadcast encryption, indistinguishability obfuscation (iO), and many others. It has been shown that a cryptographic trilinear map is sufficient for the application to iO. Dan posed the construction of such a map as a key challenge for the participants.

2.3 Ming-Deh Huang: Trilinear maps for cryptography.

The talk presented the approach discussed in [11] to constructing a cryptographic trilinear map using principally polarized abelian surfaces A over the algebraic closure of a finite field. The map has the form

$$A[\ell] \times A[\ell] \times NS(A)/\ell NS(A) \to \mu_\ell$$

where $A[\ell]$ is the ℓ-torsion of A for a large prime ℓ and $NS(A)$ is the Neron Severi group of A. This map can be interpreted as a cup product in étale cohomology, and it can be quickly computed given enough data on the arguments. The main challenge discussed at the meeting was to represent elements in $NS(A)$ in a way that makes the discrete-log problem difficult.

2.4 Peter Stevenhagen: A reciprocity law for Redei symbols.

This talk concerned the possibility of constructing cryptographically useful trilinear maps using generalizations of the Redei symbol [16]. The Redei symbol is a concrete trilinear map defined on suitable triples (a, b, c) of elements of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. The talk focused on formulas for this symbol and its properties and applications. One property is that the value of the symbol does not change if one permutes the arguments a, b and c. An application is to understanding the Galois group of the maximal pro-2 extension of $\mathbb{Q}$ that is unramified outside a given set of primes. The participants of the workshop focused after the talk on connections between the Redei symbol and Massey products (see [9], for example).

2.5 David Jao: Isogeny based crypto.

The talk surveyed the burgeoning area of isogeny-based cryptography. David explained the different flavors of the available schemes, using ordinary and supersingular elliptic curves. David also described the subexponential time quantum attack on the isogeny problem on ordinary curves.

2.6 Ted Chinburg: Background on the cohomological point of view.

This talk focused on two potential constructions of cryptographic trilinear maps via étale cohomology. The first involved using work of Skorobogatov and Zarhin in [18] to replace the group $NS(A)/\ell NS(A)$ in Huang's talk by the larger group $H^2(A, \mu_\ell)$. The main open question is to specify elements of $H^2(A, \mu_\ell)$ without encountering discrete log problems of the kind associated to $NS(A)/\ell NS(A)$. The other construction discussed in the talk was the trilinear cup product map

$$H^1(C, \mathbb{Z}/\ell) \times H^1(C, \mu_\ell) \times H^1(C, \mu_\ell) \to H^3(C, \mu_\ell^{\otimes 2}) = \mu_\ell$$

associated to a curve C over a finite field. Work of McCallum and Sharifi [13] leads to an inefficient algorithm for computing this map. The possibility of using modular forms to compute it efficiently was discussed.

2.7 Amit Sahai: Multilinear maps and obfuscation.

The talk explained why indistinguishability obfuscation (iO) is such a useful mechanism in cryptography. It also described at a high level why multilinear maps are useful for constructing an iO obfuscator.

2.8 Dan Boneh: Candidate multilinear maps from ideal lattices, and attacks.

The talk looked at current proposals for multilinear maps based on hard problems on lattices. The GGH13 and CLT13 constructions fall in this category. The talk also explained why these constructions, in their basic form, are insecure.

3 Working groups

In addition to formal lectures, we had moderated Open Problems sessions in which the participants suggested problems that might be of interest, including some to be worked on during the week. The participants then split up into working groups to work on some of these problems. We also had sessions in which representatives of the working groups gave progress reports on the results obtained to that point. Moderators for the Open Problems and Interim Reports sessions included Kiran Kedlaya and Steven Galbraith.

The working group topics included:

- Multiparty key agreement based on isogenies on abelian varieties.
- Trilinear maps via Neron-Severi groups and abelian surfaces.
- Trilinear maps via curves over finite fields, Brauer groups, and Massey and Redei symbols.
- Quantum algorithms to solve isogeny problems.
- Hilbert's 10th problem over the rational numbers.
- The local pseudo-random number generator problem.

4 Extracurricular activities

The participants also attended a public lecture on Escher and the Droste Effect by Hendrik W. Lenstra, Jr. on Tuesday evening, and a piano performance "88 Public Keys" on mathematical themes related to the workshop topic by Noam D. Elkies on Thursday evening.

5 Schedule

The schedule of the workshop allowed for ample discussions among the participants. This was appreciated by everyone.

Sunday, May 6

16:00	Check-in begins (Front Desk - Professional Development Center - open 24 hours)
17:30 - 19:30	Buffet Dinner, Sally Borden Building
20:00	Informal gathering (Corbett Hall, 2nd floor lounge)

Monday, May 7

7:00 - 9:00	Breakfast
9:05 - 9:20	Introduction and welcome by BIRS station manager
9:20 - 9:30	A. Silverberg: *Welcome by workshop organizers.*
9:30 - 10:00	A. Silverberg: *Introduction to cryptographic multlinear maps.*
10:00 - 10:30	Coffee break
10:30 - 12:00	D. Boneh: *Background on multilinear maps, and applications.*
12:00 - 13:00	Lunch
13:00 - 14:00	Guided Tour of The Banff Centre (meet in the 2nd floor lounge, Corbett Hall)
14:00 - 14:20	Group Photo
14:20 - 15:20	M-D. Huang: *Trilinear maps for cryptography.*
15:20 - 16:00	Coffee break
16:00 - 18:00	Open problems session
18:00 - 19:30	Dinner

Tuesday, May 8

7:00 - 9:30	Breakfast
9:00 - 9:50	P. Stevenhagen: *A reciprocity law for Redei symbols.*
10:30 - 11:00	Coffee break
11:00 - 12:00	*Discussion about splitting into working groups.*
12:00 - 13:30	Lunch
13:30 - 14:30	D. Jao: *Isogeny based crypto.*
14:30 - 15:00	Coffee break
15:00 - 17:30	Working groups
17:30 - 19:30	Dinner

Wednesday, May 9

7:00 - 9:00	Breakfast
9:00 - 10:00	T. Chinburg: *Background on cohomological point of view.*
10:00 - 10:30	Coffee break
10:30 - 11:30	A. Sahai *Multilinear maps and obfuscation.*
11:30 - 13:30	Lunch
	Free Afternoon
17:30 - 19:30	Dinner

Thursday, May 10

7:00 - 9:00	Breakfast
9:30 - 10:30	Working groups
10:30 - 11:00	Coffee break
11:00 - 12:00	Open problems Session II
12:00 - 13:30	Lunch
13:30 - 14:00	Woirking groups
14:00 - 14:30	D. Boneh: *Candidate multilinear maps from ideal lattices, and attacks.*
14:30 - 15:00	Coffee break
15:00 - 18:00	Working groups
17:30 - 19:30	Dinner

Friday, May 11

7:00 - 9:00	Breakfast
9:00 - 10:00	Working groups
10:00 - 10:30	Coffee break
10:30 - 11:45	Reports of working groups
11:30 - 12:00	Checkout by Noon (Front Desk - Professional Development Centre)
12:00 - 13:30	Lunch
13:00 - 14:00	T. Chinburg: *Redone video of the talk given on May 9. The video of the May 9 talk did not record.*

6 Participants

The participants of the workshop and their affiliations at the time of the workshop were as follows.

Bleher, Frauke	University of Iowa
Boneh, Dan	Stanford University
Bright, Martin	Universiteit Leiden
Chinburg, Ted	University of Pennsylvania
Elkies, Noam D.	Harvard University
Galbraith, Steven	University of Auckland
Gangl, Herbert	Durham University
Glass, Darren	Gettysburg College
Guy, Richard	The University of Calgary
Heninger, Nadia	University of Pennsylvania
Huang, Ming-Deh	USC
Jao, David	University of Waterloo
Kedlaya, Kiran	University of California, San Diego
Lee, Changmin	Seoul National University
Lenstra, Hendrik	Universiteit Leiden
Pellet–Mary, Alice	LIP, ENS de Lyon
Rubin, Karl	University of California, Irvine
Sahai, Amit	UCLA
Scheidler, Renate	University of Calgary
Scherr, Zach	Bucknell University
Shani, Barak	University of Pennsylvania
Sharif, Shahed	CSU San Marcos
Silverberg, Alice	University of California, Irvine
Stange, Katherine	University of Colorado Boulder
Stevenhagen, Peter	Universiteit Leiden
Takashima, Katsuyuki	Mitsubishi Electric / Kyushu University

Tibouchi, Mehdi	NTT Corporation
Tran, Ha	University of Calgary
Zobernig, Lukas	The University of Auckland

References

[1] Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. Contemporary Mathematics 324(1), 71–90, 2003.

[2] Dan Boneh and Mark Zhandry. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In CRYPTO 2014, pages 480–499, 2014.

[3] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. Invent. Math. 8 238–243, 1969.

[4] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654, September 2006.

[5] Luca De Feo, David Jao and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Mathematical Cryptology 8, 209–247, 2014.

[6] Gerhard Frey. On the relation between Brauer groups and discrete logarithms. Tatra Mt. Math. Publ. 33, 199–227, 2006.

[7] Gerhard Frey. Discrete logarithms, duality, and arithmetic in Brauer groups. In Algebraic geometry and its applications, volume 5 of Ser. Number Theory Appl., pages 241–272. World Sci. Publ., Hackensack, NJ, 2008.

[8] Steven D. Galbraith. Authenticated key exchange for SIDH. Cryptology ePrint Archive: Report 2018/266, `https://eprint.iacr.org/2018/266`.

[9] J. Gärtner. Rédei symbols and arithmetical mild pro-2-groups. Ann. Math. Québec 38, 13–36, 2014.

[10] Sanjam Garg, Craig Gentry, and Shai Halevi. Candidate Multilinear Maps from Ideal Lattices. In Advances in Cryptology — EUROCRYPT 2013, volume 7881 of Lecture Notes in Computer Science, 1–17, 2013.

[11] Ming-Deh A. Huang. Trilinear maps for cryptography. 2018 preprint, `https://arxiv.org/abs/1803.10325`.

[12] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. J. Cryptology, 17(4), 263–276, 2004.

[13] W. McCallum and R. Sharifi. A cup product in the Galois cohomology of number fields. Duke Math. J. 120, no. 2, 269–310, 2003.

[14] A. Menezes, T. Okamoto, S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory **39**, 1639–1646, 1993.

[15] David B. Mumford. On the equations defining abelian varieties. I. Inventiones Mathematicae 1(4), 287–354, 1966.

[16] L. Rédei, Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper I. J. Reine Angew. Math. 180, 1–43, 1939.

[17] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing, SCIC 2000-C20, Okinawa, Japan, 2000.

[18] A. Skorobogatov and Yu. Zarhin. A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces. J. Algebraic Geometry 17, 481–502, 2008.