Mathematics and Cryptography: A Marriage of Convenience?

Invited Lecture

Alice Silverberg*

Departments of Mathematics and Computer Science
University of California, Irvine
Irvine, CA, USA
asilverb@uci.edu

Abstract. Mathematics and cryptography have a long history together, with the ups and downs inherent in any long relationship. Whether it is a marriage of convenience or a love match, their progeny have lives of their own and have had an impact on the world. This invited lecture will briefly recall some high points from the past, give speculation and encouragement for the future of this marriage, and give counseling on how to improve communication, resolve conflicts, and play well together, based on personal experience and lessons learned.

1 Introduction

For a number of years, I have been moving within and between the overlapping mathematics and cryptography communities. My background is in number theory, and I became intrigued with cryptography after elliptic curves were introduced to the field. My cryptography-related research includes work on traitor tracing, hierarchical identity based encryption, bilinear and multilinear maps, torus-based cryptography, efficient use of elliptic curves and abelian varieties in cryptography, primality proving, fully homomorphic encryption, and lattices. For the past seven years I've been organizing conferences and workshops designed to bring together mathematicians and cryptographers to work on cryptography questions of common interest. In the talk, I will tell some stories about my adventures, give observations based on my experiences, and share some of what I've learned that I hope will be helpful for others.

I have some specific goals and some general goals for the talk. Specific aims include recalling some of the fruitful interactions between mathematics and cryptography from the past and how they came about, discussing problems for the future, and suggesting productive ways to move forward. Many of the impediments to making full use of mathematics to solve cryptographic questions are social rather than technical. Cultural differences between the fields can lead to

* Supported in part by the Alfred P. Sloan Foundation and by National Science Foundation Grant CNS-1703321.

obstacles and misunderstanding that delay the progress of science. I will attempt to share some thoughts and ideas for how to move forward in constructive ways. I hope that some of these suggestions will also have wider applicability, to our daily lives and our interactions with others.

My more general goals come from a sense that we live in dangerous times. Communication between people is breaking down. Norms for social behavior are changing. The value systems on which we based our decisions and our lives are being called into question. We wonder whether it makes sense to continue working as before, when the problems of the world seem so weighty. In an effort to act locally while thinking globally, in the talk I plan to give some suggestions that I hope will not only help the cryptography and mathematics communities work together, but will also be useful more generally, in working with others or communicating across cultures.

Due to the (necessarily) short time frame I was given to write this paper, there are aspects I was not able to include. In particular, I apologize for the lack of careful referencing. Ideally, I would be setting a good example by giving a complete bibliography of relevant sources, and I regret not having the time to do so. I thank the many people who contributed to the research mentioned below, and I hope they will forgive me for not citing them explicitly.

2 Fruitful interactions

There is a long history of fruitful interactions between mathematics and cryptography. Much of it involves number theory, a field of mathematics that extends back thousands of years.

One of the most well known mathematical cryptosystems is RSA, from the 1970s, whose security is based on the (presumed) difficulty of factoring products of large prime numbers.

Diffie-Hellman key exchange and El Gamal encryption, while originally based on properties of finite fields and their multiplicative groups, have been extended to make use of other groups, including groups coming from elliptic curves and, more generally, abelian varieties such as Jacobian varieties of hyperelliptic curves.

Understanding and generalizing the mathematics underlying these schemes has led to torus-based cryptography, including the LUC, XTR, and CEILIDH cryptosystems. These cryptosystems can be understood in terms of certain varieties from algebraic geometry that are called algebraic tori, which are themselves generalizations of the multiplicative group of a finite field. The algorithms in these cryptosystems can be reinterpreted as compression and decompression algorithms that allow you to send shorter transmissions for the same security. On the other hand, these compression algorithms can be viewed as telling us that one actually gets less security than had been realized, for discrete log cryptography over extensions of finite fields.

The Weil pairing on elliptic curves was first used destructively in cryptography as an attack on the elliptic curve discrete log problem, and then used constructively in pairing-based cryptography. This seems to me like an area that could have progressed sooner and faster, had there been a longer and deeper tradition of mathematicians and computer scientists working more closely together on cryptographic questions. The interest in pairing-based cryptography led to the introduction into cryptography of other number theoretic pairings, such as what cryptographers call the Tate pairing or the Tate-Lichtenbaum pairing. The use in cryptography of pairings on elliptic curves also led to the construction of identity-based encryption schemes. Work on ways to use abelian varieties to make pairing-based cryptography more efficient led to compression algorithms for points on elliptic curves over a certain class of finite fields, and this in turn led to some of the torus-based cryptography and compression results in finite fields mentioned above.

Lattice-based cryptography, which hopes to survive the advent of quantum computers, comes from a field of number theory that is traditionally called the geometry of numbers. Research in this area makes use of the arithmetic and geometry of algebraic number fields. This thriving area has great potential for future interactions between mathematics and security research.

While both factoring-based cryptography and discrete log-based cryptography, including standard elliptic curve cryptography, are threatened by the potential advent of quantum computers, a possibly quantum-resistant use of elliptic curves was recently discovered. It makes use of isogenies on elliptic curves, and its security is based on the presumed difficulty of actually finding an isogeny between two elliptic curves that have one.

Permeating these themes is the power of mathematics to make or break the security of modern-day cryptography. As alluded to above, the constructive use of mathematics in cryptography has a flip side, namely mathematical cryptanalysis, which has a long history, even before mathematics was used in a serious way to build cryptosystems. As algorithms for solving mathematics problems get better and stronger, cryptography is under threat. All that is needed is a new mathematical idea, for problems that were presumed hard to suddenly become easy. This has the potential to not only make currently used cryptosystems obsolete, but also to reveal our past secrets that we had assumed were secure, potentially including financial, medical, military, or government secrets, for good or ill.

3 Looking toward the future

I believe that mathematics and cryptography are no longer just staying together for the sake of the children. They have now committed to each other and to making it work out. Where do they go from here? Next, I give a sampling of problems.

3.1 Computing on encrypted data and fully homomorphic encryption

Creating efficient and secure methods to compute on encrypted data, for example with efficient fully homomorphic encryption, is an area where mathematical ideas have been and can continue to be helpful. Efficient and secure fully homomorphic encryption would allow people to calculate aggregate statistics from collections of sensitive data from different sources while maintaining privacy. In the history of fully homomorphic encryption thus far, both the constructions and attacks make use of ideas from both cryptology and mathematics, including the theory of lattices (geometry of numbers) and algebraic number theory.

3.2 Cryptographic multilinear maps

Pairing-based cryptography uses bilinear maps, namely, maps

$$G_1 \times G_2 \to G_3$$

that are linear in each input variable, where the G_i are finite groups in which the discrete logarithm problem is believed to be hard. This necessitates the introduction of new hard problems that I would feel more comfortable with if they were better known in and carefully studied by the mathematical community.

A natural generalization is to have more than two inputs. This leads to the open problem of finding cryptographically useful multilinear maps.

The candidate multilinear maps that we have seen so far look very different from what I envisioned when I first started thinking about cryptographic multilinear maps. They don't fall neatly into the original framework. For me, this is one of a number of examples that demonstrate the richness and potential of cryptography. It is a field in which mathematicians can be surprised by the clever ideas of computer scientists, and computer scientists can make use of deep ideas from mathematics. When the two perspectives build on one another in fruitful ways, the result is pleasing.

The theory of multilinear maps is closely connected to the theory of indistinguishability obfuscation (iO). While it's tempting to want to prove that efficient indistinguishability obfuscation cannot exist, it's unlikely that we will see a proof of that soon, since an unconditional impossibility result for iO would imply that P $\neq$ NP.

3.3 Cryptography that will survive future attacks

Mathematics is useful for generating new ideas for post-quantum cryptography, i.e., cryptography that will withstand attacks by quantum computers, in addition to being useful for analyzing the security of proposed systems. Below are some areas where I think it would be helpful if there were more mathematicians looking more deeply at these questions.

Lattice-based cryptography Interesting open questions include the question of whether supposedly hard lattice problems are as hard in ideal lattices as they are in general lattices. We should be able to use more algebraic number theory to give deeper insights to help us better understand this problem.

Isogeny-based cryptography While a sufficiently good quantum computer would break classical elliptic curve cryptography, an interesting new area of research is cryptography based on the presumed difficulty of finding (high degree) isogenies between isogenous elliptic curves. As with much of public key cryptography, this is an area where a little mathematics has gone a long way. More work is needed to understand the security of the proposed schemes.

3.4 Cryptanalysis

Mathematics is especially powerful for cryptanalysis. When the security of a cryptosystem is based on the presumed difficulty of some mathematics problem, then one good mathematical idea or algorithm might suffice to break the system. I worry that security of some systems might be based largely on the lack of awareness of the "hard problem" by the mathematicians who would be most capable of breaking it. The more mathematicians work in this area, the more confident we can be in the security of systems that rely on relatively new or unfamiliar "hard problems".

4 Working well together

Cryptology and computer security would benefit from continued and greater input of mathematical ideas. I think it would be good if more mathematicians become part of the cryptography community, and if more cryptographers become part of the mathematics community. I found it easy to assimilate into the cryptography community. The community was welcoming, and was willing to explain concepts and jargon. More difficult is for computer scientists without mathematics degrees to participate in math conferences. There is room for the math community to learn how to bring others in. Each community can learn from the other.

Different groups have different cultures with regard to territoriality, giving or withholding credit, transparency, speed of publication, and choices about where to publish (for example, journals versus conference proceedings). These choices are sometimes motivated by publication pressures coming from academia, or by patents or other intellectual property or financial concerns. These cultural differences might depend in part on whether you're a mathematician, theoretical or applied computer scientist, or engineer, and on whether you work in academia, industry, or government. The incentives in your workplace might encourage you to maintain secrecy or to publicize findings, to be generous with giving credit, deserved or otherwise, or to only give limited acknowledgement to the work of others. Such differences might make it hard for people from different workplace cultures to work together, and might lead to misunderstandings or conflict.

I'm not convinced that the research that gets done under tight deadlines and page limits, with short time windows for reviewers, is better than research done carefully and correctly, with all details filled in, that reviewers have time to fully check. The mathematics community has started to borrow the deadline and page limit culture from the computer science community, but I'm not convinced that this is a good way to publish papers or encourage correct and careful research.

NTRU and braid group cryptography can perhaps be seen as illustrative examples for how better contact between the mathematics and cryptography communities might have been helpful. The usefulness of NTRU might have been recognized sooner had the communities been closer. For braid group cryptography, a succession of proposals and breaks have led some cryptographers to dismiss anything braid-related. Someone pointed out to me that if one comes up with a good cryptosystem based on braids, in order to have credibility in the crypto community it might be best to suppress the word "braid". This raises the question of whether a succession of proposals and breaks is a bad thing. On the one hand, earlier contact and better communication between proposers and cryptanalysts might lead to fewer insecure proposals. On the other hand, too cosy a relationship between proposers and cryptanalysts might not be a good thing; adversarial or competitive relationships might lead to more secure cryptosystems.

People don't like to be told what to do. I worry that if I write in the imperative, some readers will be rubbed the wrong way. However, sound bites are easy to remember. I hope you will forgive me for writing in the imperative, and will understand the below advice not as commands, but as (hopefully helpful!) suggestions.

Behave professionally Treat your colleagues respectfully, and behave professionally.

In the late 1980s I spent a year at one of IBM's research centers. Afterwards I would tell people that the main difference I noticed between IBM and academia was that at IBM, they knew the law and obeyed it. Many of the problems and conflicts that I have seen over the years could have been avoided had people simply remembered to behave professionally, legally, and ethically.

Whether you are an advisor to students, a journal editor, a reviewer of papers, a program committee member, a manager, a student, a colleague, a chair or dean, and whether or not your behavior is questioned, ask yourself: Am I behaving professionally? Am I acting ethically? Am I setting a good example for others? Is this the way I want others to treat me? Could I do better?

Mathematicians and computer scientists sometimes have different ideas about what constitutes professional and ethical behavior. When working across disciplines, one needs to navigate and negotiate the terms of the relationship.

Learn constructive ways to communicate Good communication is important not only to help cryptographers and mathematicians work well together, or more generally to help communicate across cultures; it's also useful in all our interactions. I find that it's important to keep communication channels open. Cutting off communication can close doors.

Many misunderstandings come from mistakenly thinking that you can correctly read the minds of other people, and attributing bad motives to them. If you want to know what someone is thinking or feeling, ask them. Moreover, don't assume that others are correctly reading your mind.

Avoid jargon When communicating across fields, avoid jargon, and avoid abbreviations.

It's hard for mathematicians to attend talks by computer scientists because of the unfamiliar abbreviations. "Learning with errors" has the same number of syllables as "LWE," so when you give a talk, you might as well say the words.

It's hard for computer scientists to read technical papers written by mathematicians. I think it would be helpful if mathematicians wrote more survey talks, in less technical language, in order to explain their technical papers to people outside their specialities who might be able to make use of the results.

Listen Listen, and learn from what others have to offer. Listen to different points of view.

Ask for advice. Listen to advice (solicited or otherwise) with an open mind; you don't have to follow it.

Be curious Be curious, open-minded, and open to opportunities.

It's helpful to try to see things from the point of view of the other person. Ask questions.

For every experience, good or bad, ask yourself "What can I learn from this?"

I learned the phrase "Get curious, not furious" from the book *A New Map for Relationships: Creating True Love at Home and Peace on the Planet* by Dorothie Hellman and Martin Hellman. That book makes an eloquent case for curiosity, and for not getting angry.

Be kind As Lewis Carroll wrote about Alice in *Alice's Adventures in Wonderland*, "She generally gave herself very good advice (though she very seldom followed it)." I'm much better at giving advice, than following my own advice. For most of the advice that I'm giving here, I'm still learning how to follow it, and not doing as well as I would like.

It took me a very long time to learn that being kind solves many problems, and prevents many problems. To be clear, being kind does not mean that you let other people get their way. Being kind can include enforcing boundaries, standing up for what's right, sticking up for others, and being kind to yourself.