Abstract

Is Arithmetic Geometry necessary for Public Key Cryptography?

Gerhard Frey

The main task of public key cryptography is to provide highly efficient tools to exchange keys, sign electronic messages, authenticate members of a net and, sometimes,encrypt and decrypt messages by using simple protocols with clear and easy to follow implementation rules. For many applications the basic crypto primitive is the discrete logarithm in groups, and it is the task of mathematics to provide suitable groups. After about 25 years of intensive research we can provide lists of standardized groups (NIST et al.) and so cryptographers can apply them without further knowledge. In this sense, arithmetic geometry is not necessary for cryptography.

But typically, these groups come from arithmetic geometry, and to construct them and to shape them such that they provide fast systems took the whole arsenal of this deep theory. At the same time it turned out that every constructive tool could be used as attack to some of the groups, and it is very important to describe precisely the “weak” cases. So to understand why the suggested groups are, to our best knowledge, secure needs arithmetic geometry.

In addition, the process is not finished, and we have to continue to optimize constructions and performances and to test security, and we have to expect some surprises.

In the lecture we plan to explain the relevant constructions and to show how arithmetic geometry can be used in constructive and destructive ways. In particular, we shall stress the importance of isogenies for point counting, for attacks based on Weil descent and we shall present a rather recent argument against the use of curves of genus 3.

For mathematicians the problems risen from cryptography lead to exciting developments in theoretical and algorithmic arithmetic geometry, and for cryptographers the important message from arithmetic geometry is: The range of candidates usable for cryptography is rather narrow, but there are still plenty of groups we may trust.