COMPUTABILITY AND COMPLEXITY IN ELLIPTIC CURVES AND CRYPTOGRAPHY

LILJANA BABINKOSTOVA

Cryptographic systems are divided into two categories: In *symmetric key schemes* the communicating entities first agree on keying material that is both secret and authentic. In contrast to symmetric key schemes, *public key schemes* require only that communicating entities exchange keying material that is authentic, but not secret. Each of these cryptographic categories has advantages and disadvantages. Thus, hybrid systems that benefit from the efficiency of symmetric key algorithms and the functionality of public key algorithms are very common in practical deployments of cryptography.

The two research projects offered are inspired by current commercially used symmetric key and public key crypto systems. Each of these projects involves some computational work to gather data and analytical work towards formulating general conjectures about the fundamental structures that underly these projects as well as developing new proof techniques.

Project 1: Elliptic Pair of primes

Elliptic curves have been studied by mathematicians since ancient times: Instances of the famous Bachet equation $y^2 = x^3 + b$ are considered in the writings of Diophantus of Alexandria. Throughout the history of mathematics elliptic curves have inspired important problems, or have figured in the solution of important problems. The final proof of Fermat's last conjecture that the equation $x^n + y^n = z^n$ has no nonzero integer solutions x, y and z when $n > 2$ is a recent example. Lenstra's very successful factoring algorithm based on elliptic curves is another example.

Elliptic curves entered the commercial world and gained wider popularity after N. Koblitz and V. Miller independently proposed in 1985 to use elliptic curves to design public-key cryptographic systems. Intensive research on the security and efficient implementation of elliptic curve cryptography led in the 1990s to elliptic curve crypto systems being commercially accepted and deployed. Today elliptic curve groups is one of the major platforms in cryptography, and computational complexity issues regarding elliptic curve groups continue to be of fundamental interest. In particular: The security of elliptic curve based cryptographic systems is connected to the order of the elliptic curve group.

In this project we investigate elliptic curve groups generated by the equations of the form $y^2 = x^3 + b \mod p$ or $y^2 = x^3 + ax \mod p$ for integers a and b and prime number p. Call a pair (p, q) with $p < q$ prime numbers an *elliptic pair of primes* if there are integers $b_1 < p$ and $b_2 < q$ such that the elliptic curve group defined by $y^2 = x^3 + b_1$ over $\mathbb{Z}_p$ has order q while, the elliptic curve group defined by $y^2 = x^3 + b_2$ has, over $\mathbb{Z}_q$, order p.

This is an ongoing research and collaboration with an undergraduate student. Our preliminary investigation shows that for some prime numbers p there are several prime numbers q for which p and q form an elliptic pair, while for others there is

only one prime number q for which p and q form an elliptic pair. More recently we found new patterns leading to conjectural results about elliptic curve groups of prime order generated by equations of the form $y^2 = x^3 + b$. Our conjectures include: (1) Each integer $b < p$ which produces a prime order is a primitive root of p, if, and only if, exactly two such prime orders occur for the prime p; (2) If (p, q) is an amicable pair of prime numbers, then p is congruent to q modulo 4.

These experimental phenomena require closer study and eventually, mathematical proof. The students will start with generating more data that illustrate the possibilities of these phenomena. The data will be examined for clues on why these phenomena occur. Conjectures will arise from this analysis. Ultimately mathematical results, inspired by data-based observations, may be proven.

Elliptic pairs of primes have been independently discovered and investigated by J. Silverman and K. Stange, who call these *amicable pairs*. In [7] they gave a conjectural formulas for the frequency of amicable pairs. Students will also examine this and other conjectures that emerge from the Silverman-Stange data and analysis.

Project 2: New algebraic structures of Rijndael (AES)

AES is a key-iterated block cipher: It encrypts and decrypts blocks of data according to a secret key. The AES algorithm is a symmetric-key algorithm: The same key is used for both encrypting and decrypting the data. Originally called Rijndael, the AES cipher was developed by J. Daemen and V. Rijmen [3] in 1999.

AES is intended to replace DES (Data Encryption Standard) and Triple-DES, the previous NIST standard for protecting sensitive official information. AES, like DES, relies heavily on the ideas of Claude Shannon [6] and the concepts of *diffusion* and *confusion*. The aim of diffusion is to spread the influence of all parts of the inputs to a block cipher (the plaintext and the key) to all parts of the output (ciphertext). The aim of confusion is to make the relationship between the plaintext, ciphertext and key complicated.

The exploration of structural properties of a block cipher is important since it can give insights about the security the cipher. For most types of block ciphers it is common to investigate the algebraic structure of small scale variants of the cipher to provide a fully understandable framework for the analysis of the full cipher and its security. AES has a highly algebraic structure and could therefore be more vulnerable to algebraic attacks. This motivates the growing interest in investigating the structural and algebraic aspects of this cryptosystem. The cipher round transformations in AES are based on operations of the Field $\mathbb{F}_{2^8}$. Unlike for DES [1], there are no known investigation field operations other than the operations of the field $\mathbb{F}(2^8)$ as a basis for AES. One of the goals of this project is to develop a small scale variant of AES with round transformations based on the operations on fields of form $\mathbb{F}_{p^8}$, $p > 2$ and to investigate how this affect the security of the cryptosystem.

It is known that the group theoretic properties of a block cipher such as short cycles or small size of the group generated by the round transformations of the cipher heavily affect the security of the cipher. The question of whether the set of encryption functions is a group under functional composition is important: The answer "yes" implies that there exists a successful known-plaintext attack. Moreover, "yes" implies that multiple encryption is susceptible to the same attack because

multiple encryption would be equivalent to single encryption. In [2] we were able to prove that the set of encryption functions of 6-rounds DES over any finite group (not just $\mathbb{Z}_2$) do not form a group. It is still not known whether the set of AES encryptions form a group. A second point of research in this project will be to attempt to answer this question.

It is known that it is not sufficient for a block cipher to be secure if the group generated by the round functions of the cipher is large. It is important to know the actual structure of the group that is generated. It is known that both DES and AES generate the alternating group. In [2] we were able to provide conditions for which the round functions of an n-round DES over a finite group does not generate the alternating group. A third point of research in this project will be to attempt to answer this question in general in the case of AES.

References

[1] L. Babinkostova, A. Bowden, A. Kimball, and K. Williams, *Data Encryption Standard over Elliptic Curves*, (in preparation).

[2] L. Babinkostova, A. Bowden, A. Kimball, and K. Williams, *Data Encryption Standard over Finite Groups*, (in preparation).

[3] J. Daemen and V. Rijmen, *The Design of Rijndael*, **Springer-Verlag**, 2002.

[4] S. Landau, *Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption*, **American Mathematical Monthly**, Volume 11, Number 2, 2004.

[5] S. Murphy, K.G. Paterson, P. Wild, *A weak cipher that generates the symmetric group*, **Journal of Cryptology**, Volume 7 , 6165, 1994.

[6] C.E. Shannon, Communication Theory of Secrecy Systems, **Bell System Technical Journal**, 28-4: 656 - 715, 1949.

[7] J. Silverman, K. Stange, Amicable pairs and aliquot cycles for elliptic curves, **Experimental Mathematics**, Volume 20, Issue 3, 329-357, 2011.