# Algebraic Geometry in Cryptography

Wiesław Maleszewski

wmaleszewski@pja.edu.pl

POLISH-JAPANESE ACADEMY
OF INFORMATION TECHNOLOGY

## Introduction

The paper presents application of algebraic geometry in cryptography. In the first part we go from basic issues, among other things, such as elliptic curves, then get to know the various cryptographic systems based on elliptic curves. At the end we show some examples of applications of these methods to protect the information used in the modern world.

For millennia, rulers needed efficient and secure communication systems to efficiently govern their countries and command their armies. The danger of intercepting messages by unauthorized persons was the main motive of devising ciphers and codes. The ability to encrypt well, or to break ciphers, often influenced the course of events. Often cited an example is the story of Mary Stuart, where encryption was of little avail, because the messenger was a double agent, who passed all the correspondence (including the encryption key) to the minister the English Court, which eventually led to the beheading of the authoress.

The beginnings of cryptography date back to ancient times. It was already the ancient Egyptians who encrypted their hieroglyphs, and so did also the ancient Hebrews encrypting some words in their scripts. One of the most famous ways to encrypt information is the Caesar cipher.

A lot of encryption systems that use mechanical devices were developed in the first half of the 20th century. These systems were used, among other things, during the Second World War. Some of them, such as the German Enigma system broken by three Polish mathematicians, i.e. Marian Rejewski, Jerzy Rozycki and Henryk Zygalski, were effectively broken.

For centuries, the language barrier was an important factor supporting the power of ciphers. Due to its specificity, none of the codes based on the languages of native Americans has ever been broken, although US troops often used such codes, especially during the war with Japan.

## Review of the literature

The development of electronics in the 20th century provided tremendous opportunities to perform computing operations at a relatively low cost, which contributed to fast development in the field of designing encryption systems.

For several years, the asymmetric cryptography technique, also called elliptic curve cryptography (ECC), has enjoyed great popularity. The security of ECC is based on the computational complexity of discrete logarithms on elliptic curves (ECDLP = Elliptic Curve Discrete Logarithm Problem). Currently, it is the use of conic curve cryptography that is of special interest and importance in order to increase the protection of information systems based on computationally difficult problems.

However, more and more advanced work on the construction of quantum computers indicates the need for a new approach to information protection. Currently used methods are based on computationally difficult problems, such as e.g. the problem of factorization of large numbers or the discrete logarithm problem, which problems will be handled very well by quantum computers. Individuals and institutions involved in cryptography have a duty today to seek new methods of information protection, which will also be effective in the era of quantum computers. Particularly noteworthy, therefore, are the so-called post-quantum algorithms which are likely to find application in the era of quantum computers. They are based on, inter alia, the hash function based on the hash table (hash-based cryptography), line codes (code-based cryptography), lattice theory (lattice-based cryptography), and polynomials of the second degree of multiple variables (multivariate-quadratic-equations cryptography).

The methods based on lattice theory, which has numerous applications in quantum physics being the "older sister" of quantum computing, appear to be particularly promising. The arrival of quantum computers will also mark the end of modern cryptography based on computationally difficult problems, which is why the development of quantum cryptography is so important for the protection of transmission and collection of information in the future.

## Elliptic curves

The name of elliptic curves which appears in cryptography is slightly misleading. It is connected with the problem of determining the arc length of an ellipse using the so-called elliptic integral of the second kind. These integrals are called elliptic integrals and cannot be expressed using elementary functions. Functions inverse to elliptic integrals are called *elliptic functions*.

**Example 1.** *One of elliptic integrals is the function:*

$$u = \int_y^\infty \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}} \tag{1}$$

*A function inverse to it is the Weierstrass elliptical function $y = \wp(u)$, which satisfies the dependence:*

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3.$$

The elliptic function satisfies the equation of a curve. It is for this reason that this curve is called an *elliptic curve*.

## EC in Euclidean spaces

Let us call the elliptic curve in $\mathbb{R}^2$ as a set of solutions of the Weierstrass equation:

$$y^2 = x^3 + ax + b \tag{2}$$

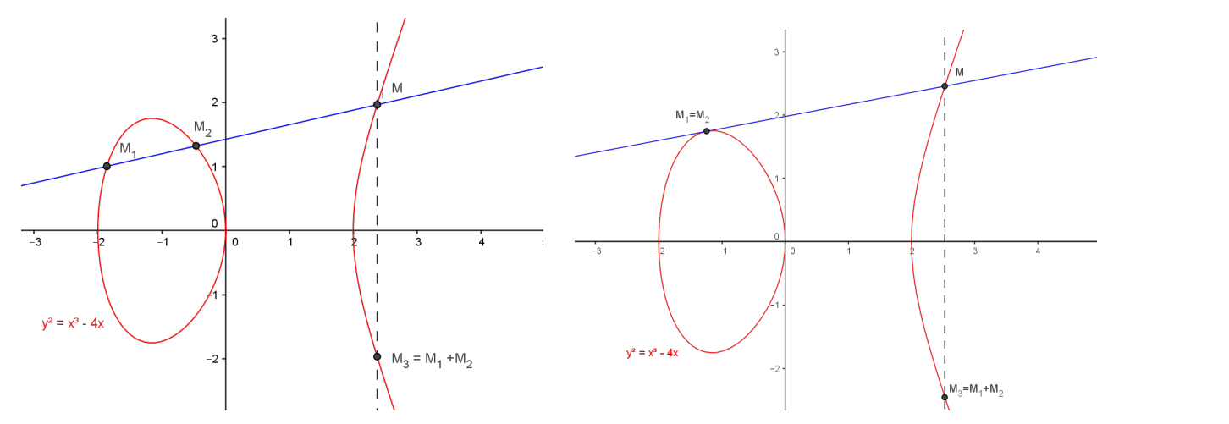
together with a point at infinity O where the constants $a$,$b$ meet the additional condition: $4a^3 + 27b^2 \neq 0$. We mark the set of solutions as $E(\mathbb{R})$. Thus, the elliptic curve is a set of:

$$E(\mathbb{R}) = \left\{(x, y) \in \mathbb{R}^2 : y^2 = x^3 + ax + b\right\} \cup \{O\}.$$

The condition $\Delta_E \neq 0$ (where $\Delta_E = -16 \cdot (4a^3 + 27b^2)$) means that the polynomial $x^3 + ax + b$ does not have multiple roots.

## The operation of "addition"

It is on elliptic curves that we can define operations of "addition". Let us take two different points $M_1$ and $M_2$ lying on the elliptic curve. In this case, the straight line passing through them intersects the curve at exactly three different points $M_1, M_2, M$. We assume that the result of adding will be point $M_3$ of the curve symmetrical to $M$, relative to the axis of abscissae.



Addition for $M_1 \neq M_2$ Addition for $M_1 = M_2$

In the case when $M_1 = M_2$, we are considering the tangent to the curve at point $M_1$, and repeat the above procedure. We encounter a problem when we want to add two points symmetrical with respect to the axis of abscissae, or double the point lying additionally on the axis of abscissae. Then, a relevant straight line assumes the position parallel to the axis of ordinates, and does not intersect the elliptic curve at any other point. The solution is to introduce point $\mathcal{O}$ called "a point at infinity".

## The algorithm of adding points on the elliptic curve (algebraic approach)

Let $E(\mathbb{R})$ be an elliptic curve, and $M_1, M_2 \in E(\mathbb{R})$, where $M_1 = (x_1, y_1)$, $M_2 = (x_2, y_2)$, and $\mathcal{O}$ is "a point at infinity", then:

- $\forall_{i,j\in\{1,2\}}(M_i \in \mathcal{O} \Rightarrow M_i + M_j = M_j)$
- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge M_j \notin \mathcal{O} \wedge x_i \neq x_j \Rightarrow M_i + M_j = (x_3, y_3))$, where:

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 (x_1 - x_3) \end{cases}$$

- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge x_i = x_j \wedge y_i = -y_j \Rightarrow M_i + M_j = \mathcal{O})$
- $\forall_{i,j\in\{1,2\}}(M_i \notin \mathcal{O} \wedge M_i = M_j \Rightarrow M_i + M_j = (x_3, y_3))$, where:

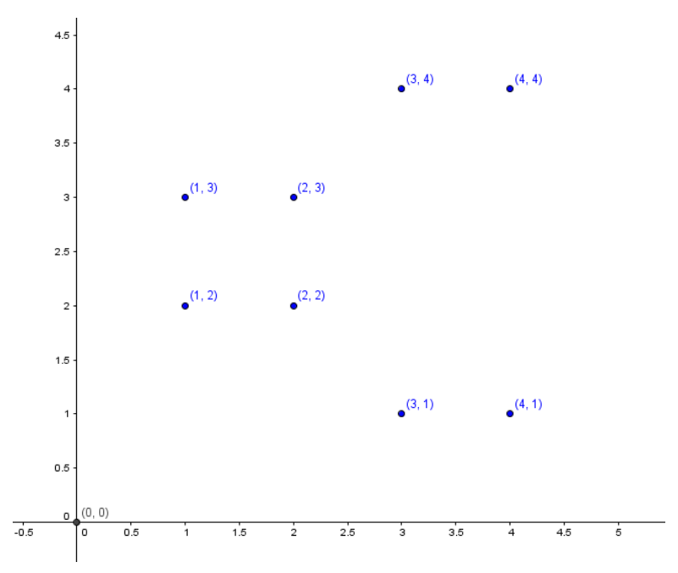
$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)^2 (x_1 - x_3) \end{cases}$$

**Remark 1.** *Remark It is easy to show that along with the aforementioned operation of "addition", and "a point at infinity", elliptic curve $E(\mathbb{R})$ is an Abelian group.*

The use of elliptic curves in the context of finite fields changes their appearance (in finite fields the diagram ceases to be a continuous curve and assumes the form of a set of points; this is a consequence of adopting a domain which is a discrete set). The method of the addition algorithm described above does not change, the only modification being that we operate in a finite field).

**Example 2.** *Let $E$ be the elliptic curve $y^2 = x^3 + 3x$ over field $F_5$. Then, curve $E$ consists of 10 points:*

$$E(F_5) = \{\mathcal{O}_E, (0,0), (1,2), (1,3), (2,2), (2,3), (3,1), (3,4), (4,1), (4,4)\}.$$



*The elliptic curve $y^2 = x^3 + 3x$ over field $F_5$.*

Let us note that the points beyond point (0,0) still retain their horizontal symmetry.

## Practical applications of elliptic curves

Starting around 1985, the theory of elliptic curves was applied to deal with a variety of cryptographic problems such as the partition of natural numbers into prime factors, tests examining whether a number is a prime number or a structure of different cryptosystems. The groups of points of elliptic curves over finite fields are similar to the multiplicative groups of finite fields. ECC algorithms provide security comparable to that of RSA with less complex keys. This provides much more efficient encryption compared to RSA, which is considered too slow and requiring considerable computing power.

## The discrete logarithm problem

One may wonder about the difficulty of finding for certain points $G, H \in E(\mathbb{K})$ such an integer $n$ that:

$$\underbrace{G + G + \ldots + G}_{n-1 \text{ additions in } E(\mathbb{K})} = [n]G = H.$$

This is the so-called discrete logarithm problem in the group of elliptic curve points. We designate the number sought as $n = \log_G H$, and say that n is a discrete elliptic logarithm with base $G$ from $H$. On the basis of knowledge of $G$ and $H$, the opponent must designate $n$, that is, solve a seemingly simple equation, whose complexity stems from the definition of the operation of addition of elliptic curve points, together with the modular arithmetic in field $F_p$. In fact, this issue is a problem extremely difficult computationally (at least for large $p$). In the case of some curves, this problem can be effectively reduced to the discrete logarithm problem in the multiplicative group of a finite field. Therefore, only those curves that meet certain conditions regarding security are selected for cryptographic applications.

## The Diffie-Hellman key exchange

A classic example of a protocol of exchanging encryption keys is the Diffie - Hellman key exchange that allows two parties to establish a secret key in an unsecured network. It does not require the knowledge of any classified information, or the presence of a trusted "third party". This protocol was the first practical solution to the problem of key distribution. It is resistant to passive attacks, but vulnerable to active ones due to the lack of transmitted information authentication keys. The security of this protocol is based on the complexity of the discrete logarithm problem.

## The ECIES encryption scheme

The Elliptic Curve Integrated Encryption Scheme (ECIES) is a static version of the Diffie-Hellman key exchange, in which the exchange of the key does not take place with the active participation of both parties to the protocol. In practice, it comes down to the fact that one of the parties provides their public key to all who would like to exchange information with them in a secure manner. The algorithm is popular mainly because of the very high prevalence of use of the Diffie-Hellman protocol. All systems implementing the ECDH (Elliptic Curve Diffie-Hellman) protocol can be adapted to support ECIES encryption, which is important in systems with limited storage resources.

## ElGamal digital signature

A mechanism to ensure the authenticity of transmitted data was presented in 1985 by ElGamal. At the core of this algorithm's operation lies the discrete logarithm problem. The algorithm allows the encryption and support of digital signatures.

Description of the algorithm

1. We select such a large enough prime number p, that the calculation of the discrete logarithm is virtually impossible.
2. We select integer $0 < a < p - 1$ and number $g$, and then calculate $b \equiv g^a \ (mod\ p)$; numbers $\{b, g, p\}$ constitute the public key, whereas numbers $\{a, g, p\}$ the private key.
3. In order to encrypt message $M$, we select random number $k$ relatively prime to number $p-1$, and then calculate $c_1 \equiv g^k \ (mod\ p)$ and $c_2 \equiv M \cdot b^k (mod\ p)$. The pair of numbers $c_1$ and $c_2$ creates a cryptogram, which is longer than the plain text.
4. Decryption consists in calculating:

$$M = c_2(c_1^a)^{-1} \ (mod\ p)$$

**Example 3.** *Let $p = 47$ and $g = 5$ , we select $a = 20$ and calculate*

$$b = g^a = 5^{20} \ (mod\ 47) = 3.$$

*Thus, numbers $\{3, 5, 47\}$ constitute the public key,*
*and numbers $\{20, 5, 47\}$ are the private key.*

*Encryption:*
*Let the message be $M = 38$. We select such $k = 11$ that $GCD(38, 11) = 1$ (this number is not disclosed),*

$$c_1 = 5^{11} \ (mod\ 47) = 13$$

*and*

$$c_2 = 38 \cdot 3^{11} \ (mod\ 47) = 11$$

*Decryption:*

$$M = c_2 \cdot (c_1^a)^{-1} \ (mod\ 47) \equiv 11 \cdot 12 (mod\ 229) = 38.$$

A special representative of the ElGamal signature is the Digital Signature Algorithm (DSA), which constitutes the basis of the Digital Signature Standard (DSS). Elliptic curve cryptography is also based on the concept of the ElGamal algorithm. In this case, instead of the multiplicative group of field $\mathbb{Z}_p$ we use the group of points on the elliptic curve.

## Security requirements

Security guaranteed by the systems in question is connected with existing algorithms serving to determine the discrete logarithm on elliptic curves. The best-known algorithms allowing to solve or significantly simplify the problem include, among others, the Pollard's rho algorithm and the Pohlig-Hellman algorithm.

## Summary

As already mentioned at the beginning of the article, new methods are needed to increase the security of information transmission. In the world using modern technology, studies in the field of number theory and algebraic geometry constitute now a mathematical foundation and, therefore, a key challenge for modern cryptography. Another very important area of research includes methods that guarantee the security of information in times of availability of quantum computers.

## Examples of applications

*National Scrambler (WAT & WASKO)*

*Bitcoin - payment system*

## References

1. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer 1991.
2. N. Koblitz, *Algebraic Aspects of Cryptography*, Springer 1997.
3. A. Chmielowiec, *Wydajne metody generowania bezpiecznych parametrow algorytmow klucza publicznego*, PAN 2012.
4. M. Jurkiewicz, J. Gawinecki, P. Bora, T. Kijko, *Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmow i protokolow kryptograficznych*, WAT 2014.
5. K. Bondaryk, J. Pomykała; *Nowe wyzwania dla polskiej kryptologii drugiej dekady XXI wieku*, WAT 2014.
6. K. Bhirud, D. Kulkarni, R. Pawar, P. Patil, *Data Security Using Elliptic Curve Cryptography*, International Journal of Computer Engineering In Research Trends, 2016.
7. S. Signh, *Ksiega szyfrow*, Albatros 2001.