Pol. J. Appl. Sci., **2016**, *2*, 11-15

ALGEBRAIC GEOMETRY IN CRYPTOGRAPHY AT THE TURN OF THE XX–XXI CENTURY

Wiesław Maleszewski

Department of Applied Informatics
Polish-Japanese Academy of Information Technology, Warsaw, Poland

E-mail: wmaleszewski@pja.edu.pl

Abstract: The paper presents the application of algebraic geometry to cryptography. In the first part we cover some basic issues, such as elliptic curves, then present 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.

Key words: elliptic curve, cryptography, ElGamal digital signature, security information, algebraic geometry

Introduction

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 for devising ciphers and codes. The ability to encrypt successfully or to break ciphers has often influenced the course of events. Often cited an example is the story of Mary Stuart, where encryption was of little help, because the messenger was a double agent, who passed all the correspondence (including the encryption key) to the minister of the English Court, which eventually led to the beheading of the author.

The beginnings of cryptography date back to ancient times. The ancient Egyptians encrypted their hieroglyphics and the ancient Hebrews also encrypted some words in their texts. 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 twentieth century. These systems were used at many times and even during the Second World War. Some of them were effectively broken, such as the German Enigma system which was broken by three Polish mathematicians Marian Rejewski, Jerzy Różycki and Henryk Zygalski.

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, even though US troops often used such codes, especially during the war with Japan [1].

Review of the literature

Fig. 1: Polish mathematicians, Marian Rejewski, Jerzy Rozycki and Henryk Zygalski.

The development of electronics in the twentieth century provided tremendous opportunities to perform computing operations at a relatively low cost, which contributed to the 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 which 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 security. The currently methods are based on computationally difficult problems, such as the problem of factorization of large numbers or the discrete logarithm problem. These problems can be handled very easily by quantum computers. Individuals and institutions involved in cryptography have a duty today to seek new methods of information protection, which will continue to be effective in the era of quantum computers. Particularly noteworthy, therefore, are the so-called post-quantum algorithms which are likely to be found in applications 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 and cannot be expressed using elementary functions. Functions inverse to elliptic integrals are called elliptic functions [2].

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 [2].

Elliptic curves 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 $\mathcal{O}$ 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 defined by the equation:

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

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 [3, 4].

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.

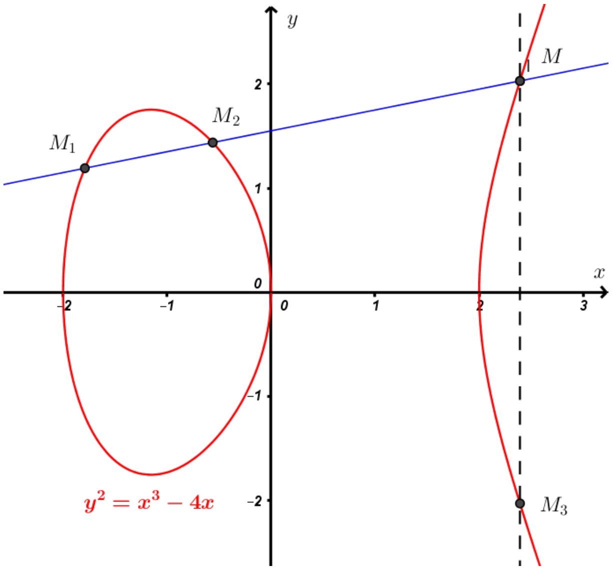

Fig. 2: Addition for $M_1 \neq M_2$.

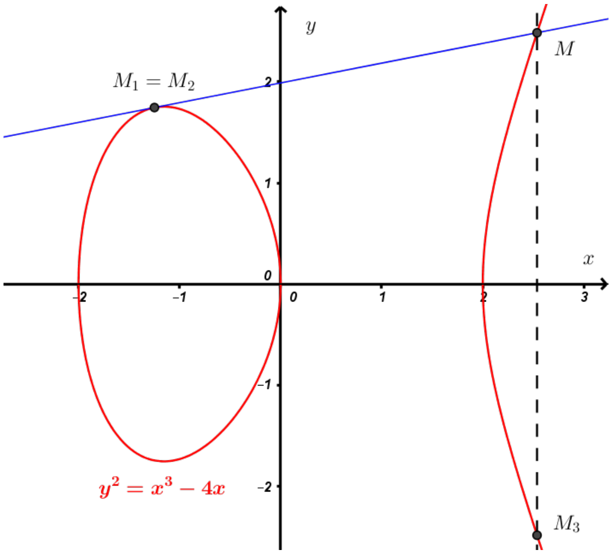

Fig. 3: Addition for $M_1 = M_2$.

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 [2]. 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" [5].

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

Let $E(\mathbb{R})$ be an elliptic curve, $M_1, M_2 \in E(\mathbb{R})$ 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

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

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

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

Remark 1: 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 additional 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 the field $F_5 = (\mathbb{Z}_5, + \pmod 5), \cdot \pmod 5))$. Then, curve E consists of 10 points:

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

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

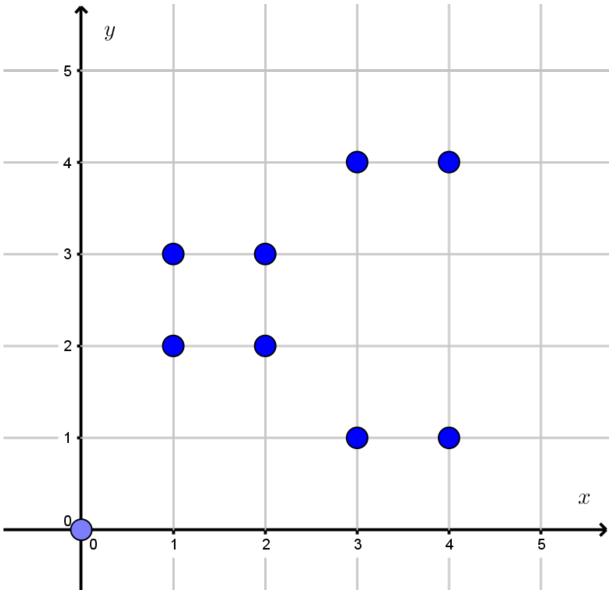

Fig. 4: The elliptic curve $y^2 = x^3 + 3x$ over field F_5.

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 requires 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:

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

This is the so-called discrete logarithm problem in the group of elliptic curve points [3]. 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 which is extremely difficult computationally (at least for large p) [6]. 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 [7].

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 [2].

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. Select such a large enough prime number p, that the calculation of the discrete logarithm is virtually impossible.
2. Select integer $0 < a < p - 1$ and number g; and then calculate $b \equiv g^a \,(\text{mod}\ p)$; 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 $c_1 \equiv g^k \,(\text{mod}\ p)$ and $c_2 \equiv M \cdot b^k \,(\text{mod}\ p)$. The pair of numbers c_1 and c_2 creates a cryptogram, which is longer than the plain text.
4. Decryption consists in calculating:

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

Example 3: Let $p = 47$ and $g = 5$. Select $a = 20$ and calculate

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

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

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

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

and

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

Decryption:

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

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, which can be solved or which can significantly simplify the problem, include Pollard's rho algorithm and the Pohlig-Hellman algorithm among others [2].

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 [4]. Another very important area of research includes methods that guarantee the security of information in times of availability of quantum computers [8].

Literature

[1] Signh S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Doubleday, 1999.

[2] Chmielowiec A. *Wydajne metody generowania bezpiecznych parametrow algorytmow klucza publicznego.* PAN, 2012.

[3] Chmielowiec A. *Współczesna kryptografia – schematy bazujące na parowaniu punktów krzywej eliptycznej.* PAN, 2010.

[4] Bondaryk K., Pomykała J. *Nowe wyzwania dla polskiej kryptologii drugiej dekady XXI wieku.* WAT, 2014.

[5] Koblitz N. *Algebraic Aspects of Cryptography.* Springer, 1997.

[6] Jurkiewicz M., Gawinecki J., Bora P., Kijko T. *Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmów i protokołów kryptograficznych.* WAT, 2014.

[7] Koblitz N. *A Course in Number Theory and Cryptography.* Springer, 1991.

[8] Gruber J., Iwanicki D., Jacak M., Jóźwiak I.J., Jóźwiak P.P., Kowalczyk J. Kryteria budowy komputera kwantowego i kryptografii postkwantowej. In *XLIII KZM Zakopane*, 2014.

Received: 2016
Accepted: 2016