Pol. J. Appl. Sci., **2018**, *4*, 96-101

THE APPLICATION OF ISOGENIC ELLIPTIC CURVES AND GRAPHS IN POST-QUANTUM CRYPTOGRAPHY

Wiesław Maleszewski

Faculty of Computer Science and Food Science
Lomza State University of Applied Sciences, Lomza, Poland

E-mail: wmaleszewski@pwsip.edu.pl

Abstract: The article presents the properties of elliptic curves and the laws of arithmetic in their structures forming an additive group characterized by relatively low computational costs of performing group operations. The concept of isogens is introduced, the structure of a quotient grid in the body of complex numbers is defined and the properties of group activities in these structures are enumerated. Next, reference was made to the methods of exchanging cryptographic keys based on graph structures. In the next part, the Supersingular Isogeny Key Exchange is introduced, and a comparison of three versions of the Diffie-Hellman key phrase protocol is made – classical, based on elliptic curves and based on isogeny. Finally, research problems were presented in the area where any minimal progress would bring a greater guarantee of secure communication – both now and in the future when quantum computers will be available.

Key words: post-quantum cryptography, elliptic curve, SIDH, IoT.

DOI: 10.34668/PJAS.2018.4.3.03

Introduction

The idea of building quantum computers was born as early as the 1980s, when Paul Benioff [1] proposed the possibility of building a machine that uses the laws of quantum physics to operate. However, it was the Nobel Prize winner, Richard Feynman, who during one of his famous lectures at the Massachusetts Institute of Technology in 1981 presented the theoretical model of transforming the quantum system into a classic computer model, he is considered to be the creator of the idea of building a quantum computer. The dynamic development of science and technology is leading to a time when quantum computers will stop being toys in the hands of scientists and become powerful tools. These tools may change the visions of world development. At the same time, the development of work on the construction of quantum computers is accompanied by an increasing interest in quantum algorithms which, based on the nonintuitive phenomena of quantum mechanics such as the superposition of states, interference of probability amplitudes, or quantum entanglement, promises the ability to solve a new class of problems.

Due to the specific properties of quantum computers, some problems currently computationally difficult can be solved in a much shorter time, which in practice can widen the scope of computer – solvable problems. A classic example of such algorithms is the Shor factorization algorithm, used for the factorization of numbers. The implementation of an algorithm that produces similar results on classical computers requires a very long time, often exceeding even the average life expectancy of a human being, while on quantum computers it can be done in such a short time that modern cryptographic algorithms based on computationally difficult problems will become useless.

Another class of algorithms designed for quantum computers are post-quantum algorithms, characterized by specific universality since they can be used in both classical and quantum computers. This universality puts them at the centre of attention of many researchers dealing with cybersecurity issues.

Description of the problem

On the one hand, the progress in the work on the construction of quantum computers is forcing scientists to deal with new algorithms resistant to attacks from quantum computers. On the other hand, the development of devices of the Internet of Things contributes to the search for algorithms that generate low computational costs of coding and decoding information.

Modern algorithms are based on so-called computationally difficult problems. One of the computationally difficult problems in the modern world is the problem of factorization. The asymmetric algorithm RSA is based on the problem and was designed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. Another computationally difficult example is the discrete logarithm problem – this is the base for Elliptic Curve Cryptography (ECC). These problems do not guarantee security against attacks from quantumdo or quantum computers. Additionally, the costs of encrypting and decrypting data in RSA are so high that the application of this algorithm in devices with limited computational resources becomes difficult.

Motivation and methodology

An optimal but at the same time very difficult solution to the defined problem is the development of a comparatively low-cost algorithm on the side of the sender and recipient of correspondence and, at the same time, one based on post- quantum problems. Such an algorithm, on the one hand, could be used in Internet of Things (IoT) devices and, on the other hand, it would provide protection making it possible to eliminate attacks made in the future using quantum computers.

Related Work

As already mentioned, the idea of building quantum computers has quite a rich history, which is why some solutions have already been developed. We can divide post-quantum cryptography algorithms, recognized today as classical, into four basic groups:

1. cryptographic algorithms based on hash tree function (hash-based cryptography); an example of such an algorithm is the public key system based on the hash tree or Merkle tree [2];
2. algorithms based on linear codes (code-based cryptography); an example of such an algorithm is the McEliece algorithm (1978), which uses Goppa codes [3];
3. cryptographic algorithms based on a lattice (lattice-based cryptography); an example is the Hoffstein-Pipher-Silverman NTRU algorithm (1998) [4];
4. algorithms based on multivariate quadratic polynomials (multivariate – quadratic – equations cryptography). An example is the HFE Patriana public key signature system (1996) [5].

The NTRU algorithm was the first algorithm of asymmetric cryptography the mathematical foundations of which simultaneously extended beyond the factorization problem and the discrete logarithm problem. Its idea is based on the shortest vector problem in a lattice. In literature, we can also find cryptographic algorithms based on the algebraic structure of a lattice defined by the relations of partial order.

In the latest literature, we can still find algorithms based on supersingular isogeny graphs that will be presented later in this work. Supersingular isogeny graphs are a class of expander graphs that have emerged in computational number theory and have been applied in elliptic-curve cryptography. Vertices represent supersingular elliptic curves over finite fields and edges represent isogenies between curves

Elliptic curves

An elliptic curve E over a field F can be given by the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients $a_i \in F$ for $i = 1, 2, 3, 4, 6$. Koblitz [6] and Miller [7] were the first to show that the group of rational points on an elliptic curve E over a finite field F_q could be used for the discrete logarithm problem in a public-key cryptosystem.

The canonical short Weierstrass form of an elliptic curve [8] is given by the equation:

$$y^2 = x^3 + ax + b,$$

together with a point at infinity $\mathcal{O}$ where the constants a, b meet the additional condition:

$$4a^3 + 27b^2 \neq 0.$$

The algorithm of adding points on the elliptic curve

Let E be an elliptic curve, and $M_1, M_2 \in E$, where $M_1 = (x_1, y_1)$, $M_2 = (x_2, y_2)$, $M_3 = (x_3, y_3)$ and $M_3 = M_1 + M_2$, [9, 10] then:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases},$$

where:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & if \quad (x_1, y_1) \neq (x_2, \pm y_2) \\ \frac{3x_1^2 + a}{2y_1} & if \quad (x_1, y_1) = (x_2, \pm y_2) \end{cases}.$$

Maps between elliptic curves

Definition 1. (j-invariant). Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, The *j-invariant* of E is given by the formula:

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Two curves are isomorphic over the algebraic closure $\bar{k}$ if and only if they have the same j-invariant [11].

Isogenies

Let $\phi : E \to E'$ be a map between elliptic curves. These conditions are equivalent:

- ϕ is a surjective group morphism,
- ϕ is a group morphism with finite kernel,
- ϕ is a non-constant algebraic map of projective varieties sending the point at infinity of E onto the point at infinity of E',

If they hold ϕ is called an ***isogeny***.

Definition 2. Two curves are called isogenous if there exists an isogeny between them.

Example 1. *Let $A, B \in \mathbb{F}_q$ be such that $B \neq 0$ and $D = A^2 - 4B \neq 0$. Consider the elliptic curve over $\mathbb{F}_q$:*

$$E : y^2 = x(x^2 + Ax + B).$$

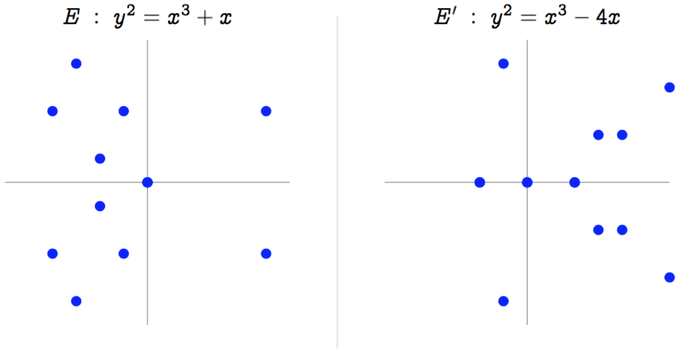
The point $(0,0)$ has order 2. There is an elliptic curve E' and an isogeny $\phi : E \to E'$ such that $ker(\phi) = \{0_E, (0,0)\}$. One can verifity that

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(B-x^2)}{x^2}\right) = \left(\frac{x^2+Ax+B}{x}, \frac{y(B-z^2)}{x^2}\right)$$

has the desired kernel [12], and the imagine curve is

$$E' = Y^2 = X(X^2 - 2AX + D).$$

Example 2. *Another example of isogeny over $\mathbb{F}_{11}$ is shown in the next figure:*


$E\ :\ y^2 = x^3 + x$

$E'\ :\ y^2 = x^3 - 4x$

Fig. 1: $\phi(x,y) = \left(\frac{x^2+1}{x}, y\frac{x^2-1}{x^2}\right)$

Definition 3. (Supersingular isogeny problem) Given a finite field K and two supersingular elliptic curves E, E' defined over K such that $|E| = |E'|$, compute an isogeny $\phi : E \to E'$ [13].

Definition 4. (Complex lattice) A complex lattice Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}-$basis. Explicitly, a complex lattice is generated by a basis (ω_1, ω_2), such that $\omega_1 \neq \Lambda\omega_2$ for any $\Lambda \in R$, as

$$\lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}.$$

Definition 5. (Complex torus). Let Λ be a complex lattice, the quotient C/Λ is called a *complex torus.*

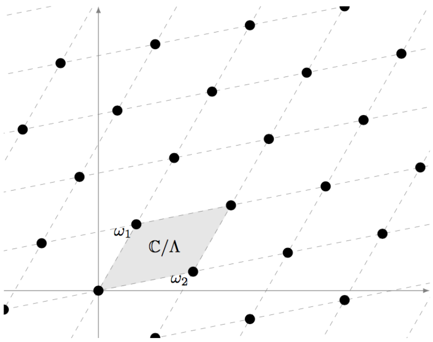


Fig. 2: A complex lattice (black dots) and its associated complex torus (grayed fundamental domain)

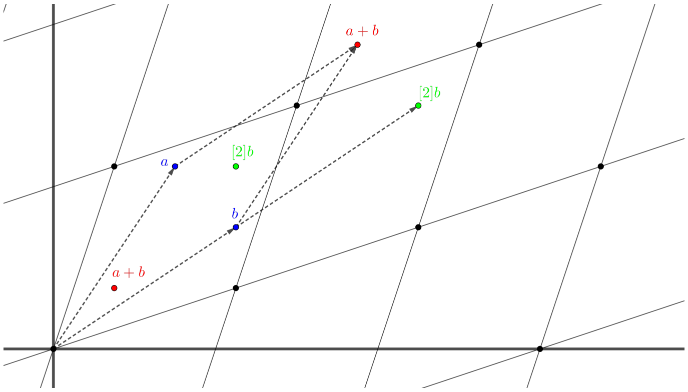


Fig. 3: Addition and scalar multiplication in a complex lattice

Definition 6. An Expander graph is a sparsely populated graph that is well connected [14].

Key exchange from Schreier graphs

Public parameters:

- A group $G = \langle g \rangle$ of order p;
- A subset $S \subset (\mathbb{Z}/p\mathbb{Z})^x$.

1. Alice takes a secret random walks $S_A : g \to g_A$ of length $O(\log p)$;
2. Bob does the same;
3. They publish g_A and g_B;
4. Alice repeats her secret walk s_A starting from g_B. Bob repeats his secret walk s_B starting from g_A.

Definition 7. A sparse graph is a graph in which the total number of edges is few compared to the maximal number of edges [14].

Example 3. *Consider a simple graph G with n vertices and 2 edges originating from each vertex. There are $2n$ edges in this graph. If this graph was a complete graph, every vertex connected to every other vertex, we would need $n!$ edges. It is clear that this graph is sparse since $n! \gg 2n$.*

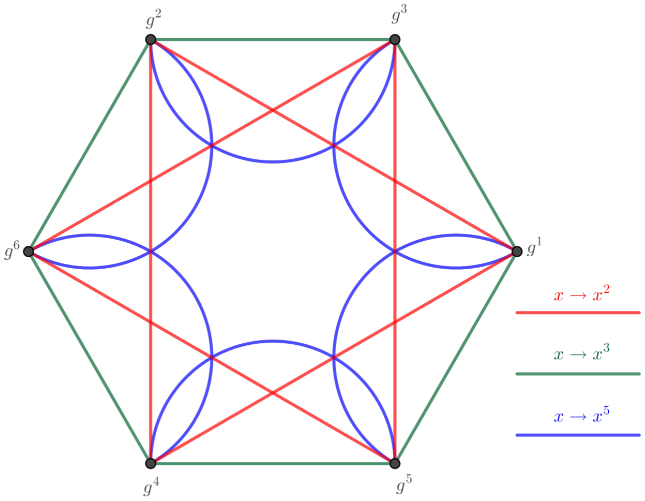


Fig. 4: The Schreier graph of $(S; G \setminus \{1\})$, where $G = \langle g \rangle$, $ord(g) = 7$.

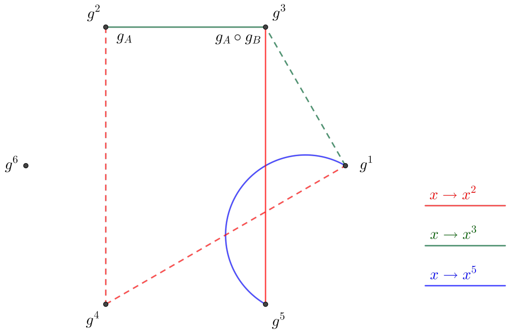


Fig. 5: Key exchange from Schreier graphs $g_A \circ g_B = (g^{5\cdot 2\cdot 3}) \circ (g^{2^2\cdot 3}) = g^{5\cdot 2^3\cdot 3^2}$

Supersingular isogeny Diffie-Hellman key exchange (SIDH)

Supersingular isogeny Diffie-Hellman key exchange (SIDH) is a post-quantum assymetric cryptographic algorithm. Out of all post-quantum key exchanges, SIDH uses the smallest keys; with compression, SIDH uses 2688- bit public keys at a 128-bit quantum security level. These properties make this protocol a natural candidate to replace Diffie Hellman (DHE) and elliptic curve Diffie Hellman (ECDHE), which are widely used in Internet communication [15]. Let ℓ_B and ℓ_B be two small prime, f be integer cofactor and let p be a prime such that:

$$p = \ell_A^{eA} \ell_B^{eB} f \pm 1.$$

For $\ell \in \{\ell_A, \ell_B\}$ and $e \in \{e_A, e_B\}$ the corresponding exponent, we have that the full ℓ^e- torsion group on E is defined over $\mathbb{F}_{p^2}$. Since ℓ is coprime to p this

$$E[\ell^e] \cong (\mathbb{Z}/\ell^e\mathbb{Z}) \times (\mathbb{Z}/\ell^e\mathbb{Z}).$$

Let $P, Q \in E(\ell^e)$ be two points that generate $E(\ell^e)$ such that the above isomorphism is given by:

$$(\mathbb{Z}/\ell^e\mathbb{Z}) \times (\mathbb{Z}/\ell^e\mathbb{Z}) \to E[\ell^e]$$

and described by the formula:

$$(m, n) \to [m]P + [n]Q.$$

The public parameters are the supersingular curve E_0/F_{p^2} whose group order is $(\ell_A^{eA} \ell_B^{eB} f)^2$, two independent points P_A and Q_A that generate $E_0[\ell_A^{eA}]$, and two independent points P_B and Q_B that generate $E_0[\ell_B^{eB}]$. To compute public key, Alice chooses two secret integers

$$m_A, n_A \in \mathbb{Z}/\ell_A^{eA}\mathbb{Z},$$

not both divisible by ℓ_A, such that

$$R_A = [m_A]P_A + [n_A]Q_A$$

has order ℓ_A^{eA}. Her secret key is computed as the degree ℓ_A^{eA} isogeny:

$$\phi_A : E_0 \to E_A$$

whose kernel is R_A, and her public key is the isogenous curve E_A together with the image points $\phi_A(P_B)$ and $\phi_A(Q_B)$. Similarly, Bob chooses two secret integers $m_B, n_B \in \mathbb{Z}/\ell_B^{eB}\mathbb{Z}$ not both divisible by ℓ_B , such that:

$$R_B = [m_B]P_B + [n_B]Q_B$$

has order ℓ_B^{eB}. He then computes his secret key as the degree

$$\phi_B : E_0 \to E_B$$

whose kernel is R_B, and his public key is E_B together with $\phi_B(P_A)$ and $\phi_B(Q_A)$. To compute the shared secret, Alice uses her secret integers and Bobs public key to compute the degree ℓ_A^{eA} isogeny $\phi_A^{'} : E_B \to E_{BA}$ whose kernel is the point:

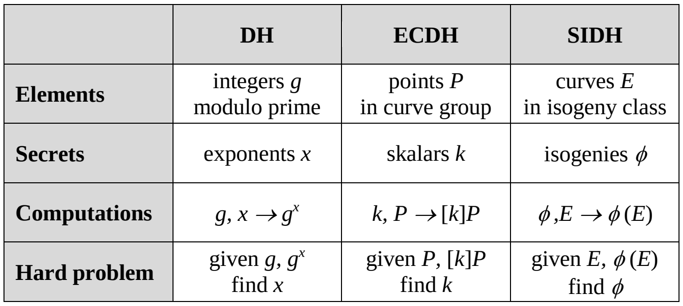
$$[m_A]\phi_B P_A + [n_A]\phi_B Q_A = \phi_B([m_A]P_A + [n_A]Q_A) = \phi_B Q_A.$$

Similarly, Bob uses his secret integers and Alice's public key to compute the degree ℓ_B^{eB}. isogeny $\phi_B^{'} = E_B \to E_{AB}$ whose kernel is the point

$$[m_B]\phi_A P_B + [n_B]\phi_A Q_B = \phi_A Q_B$$

It follows that E_{BA} and E_{AB} are isomorphic, so Alice and Bob can compute a shared secret as the common j-invariant $j(E_{BA}) = j(E_{AB})$ [17–19].
The following table shows a comparison of asymmetric algorithms:

Table 1: Comparison of Diffie-Hellman algorithms[16]



	DH	ECDH	SIDH
Elements	integers g modulo prime	points P in curve group	curves E in isogeny class
Secrets	exponents x	skalars k	isogenies ϕ
Computations	$g, x \to g^x$	$k, P \to [k]P$	$\phi, E \to \phi(E)$
Hard problem	given g, g^x find x	given P, $[k]P$ find k	given E, $\phi(E)$ find ϕ

Current isogeny problems

Researchers working in this area indicate the following research problems [20–22]:

1. **Isogeny computation** Given an elliptic curve E with Frobenius endomorphism π, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the rational fractions and the image curve of the separable isogeny $\phi : E \to E/G$.
2. **Explicit isogeny** Given two elliptic curves E, E' over a finite field, isogenous of known degree d, find an isogeny $\phi : E \to E'$ of degree d .
3. **Isogeny walk** Given two elliptic curves $E; E_0$ over a finite field k,such that $\#E = \#E'$, find an isogeny $\phi : E \to E'$ of smooth degree.

Summary

Security of communication is very important in the modern world, in which cryptography is no longer the domain of only armies and agents, but it serves directly the general public – ensuring secure communication on the Internet or enabling the functioning of modern payment systems. Cryptography helps build a more trusted world. When uquantum computers appear, many modern methods of i information protection will lose their power, and we will be forced to use newer coding techniques such as, for example, the SIDH algorithm. Its safety is connected, among others, with the problem of finding isogenic mapping between two supersingular elliptical curves. The research is aimed at formulating algebraic properties that reduce the difficulty of this problem.

Literature

[1] Benioff P. *The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines.* Journal of statistical physics, 22(5), pp.563-591, 1980

[2] Becker G. *Merkle signature schemes, merkle trees and their cryptanalysis.* Ruhr-University Bochum, Tech. Rep., 2008

[3] Mceliece R.J. *A public-key cryptosystem based on algebraic.* Coding Thv, 4244, pp.114-116, 1978

[4] Hoffstein J., Pipher J., Silverman J.H *TRU: A ring-based public key cryptosystem.* In International Algorithmic Number Theory Symposium, Springer (pp. 267-288), 1998

[5] Kipnis A., Shamir A. *Cryptanalysis of the HFE public key cryptosystem by relinearization.* In Annual International Cryptology Conference, Springer, (pp. 19-30), 1999

[6] Koblitz N. *Elliptic curve cryptosystems.* Mathematics of computation, 48(177):203-209, 1987

[7] Miller V.S. *Use of elliptic curves in cryptography.* In Conference on the Theory and Application of Cryptographic Techniques, pp. 417-426, Springer, 1985

[8] Maleszewski W. *Algebraic Geometry in Cryptography at the turn of the XX-XXI Century*, Polish Journal of Applied Sciences 2(1) pp. 11 - 15, 2017

[9] Liu Z., Großsächdl J., Hu Z., Järvinen K., Wang H., Verbauwhede I. *Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things.* IEEE Transactions on Computers, 66(5): 773-785, 2017

[10] Sughasiny M. *Give-and-take key processing for Cloud-linked IoT.* International Journal on Future Revolution in Computer Science and Communication Engineering (Vol. 3).

[11] De Feo L. *Mathematics of Isogeny Based Cryptography*, arXiv preprint arXiv:1711.04062, 2017.

[12] Galbraith S.D., Vercauteren F. *Computational problems in supersingular elliptic curve isogenies*, Quantum Information Processing, 17(10), p 265, 2018

[13] Galbraith S.D., Petit C., Shani B., Ti Y.B. *On the security of supersingular isogeny cryptosystems*, In International Conference on the Theory and Application of Cryptology and Information Security, pp. 63-91. Springer, 2016

[14] Shlomo H., Linial N., Wigderson A. *Expander graphs and their applications* Bulletin of the American Mathematical Society 43(4): 439-561, 2006

[15] https://en.wikipedia.org/wiki/Supersingular˙isogeny˙key˙exchange

[16] Costello C. *An introduction to supersingular isogeny-based cryptography.* ECC 2017 Nijmegen https:

//ecc2017.cs.ru.nl/slides/ecc2017school-costello.pdf, 2017

[17] Costello C., Longa P., Naehrig M. *Efficient algorithms for supersingular isogeny Diffie-Hellman*, In Annual Cryptology Conference (pp. 572-601), 2016.

[18] Jao D., De Feo L. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies* International Workshop on Post-Quantum Cryptography (pp. 19-34). Springer, 2011

[19] Galbraith S.D. *Authenticated key exchange for SIDH*, 2018

[20] Maleszewski W. *Analysis of the certain cryptographic problems in protocols of certyfing the nodes in IoT infrastructure* Polish Journal of Applied Sciences, 3(4), pp.141-145, 2017

[21] Petit C., Lauter K. *Hard and easy problems for supersingular isogeny graphs*, Cryptology ePrint Archive, Report 2017/962 http://eprint.iacr.org/2017/962, 2017

[22] De Feo L. *Isogeny graphs in cryptography* http://defeo.lu/docet/talk/2018/05/31/gdr-securite, 2018

Received: 2018
Accepted: 2018