A combinatorial approach to modern cryptography...

Wiesław Maleszewski
Department of Computer Science and Programming
Faculty of Computer and Food Sciences
Lomza State University of Applied Sciences
wmaleszewski@pwsip.edu.pl

Abstract

In this paper, we discuss modern cryptographic systems dedicated to sensor network that bases its functioning on combinatorial problems.

1. 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 $a_i \in E$ for $i = 1, 2, 3, 4, 6$. Koblitz [1] and Miller [2] 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 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 $M_3 = M_1 + M_2$, [3, 4] then:

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

where:

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

2. 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.

3. 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 *Isogenies: an example over $\mathbb{F}_{11}$*

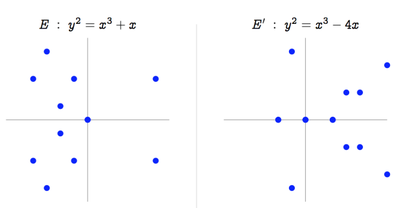

Figure 1: $\phi(x, y) = \left(\frac{x^2+1}{x}, y\frac{x^2-1}{x^2}\right)$

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 $\phi : E \to E'$ [5].*

Definition 4 *(Complex lattice) A complex lattice Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis [7].*

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 [7].*

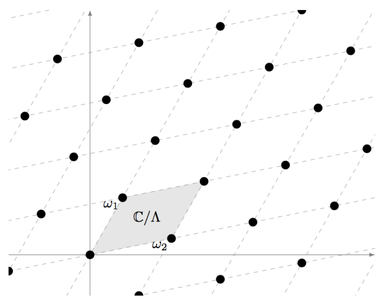

Figure 2: *A complex lattice (black dots) and its associated complex torus (grayed fundamental domain)*

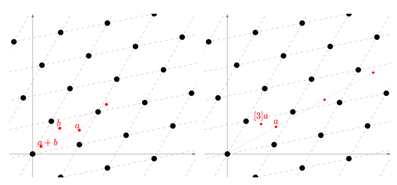

Figure 3: *Addition and scalar multiplication*

Definition 6 *An Expander graph is a sparsely populated graph that is well connected [8].*

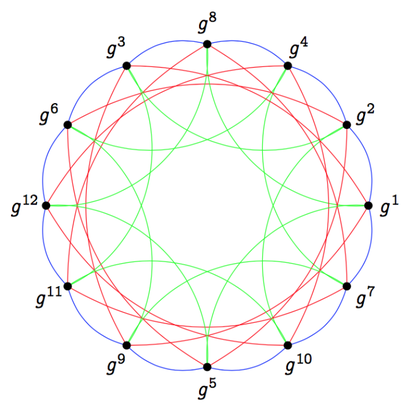

Figure 4: *The Schreier graph of $(S; G\backslash\{1\})$, where $G = \langle g \rangle$, $ord(g) = 13$*

4. Key exchange from Schreier graphs

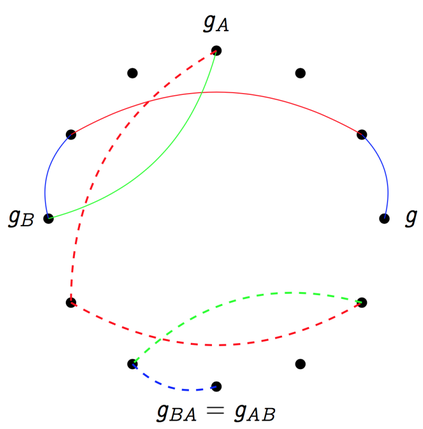

Figure 5: $g_A = g^2 \cdot 3 \cdot 2 \cdot 5$; $g_B = g^{3^2 \cdot 5 \cdot 2}$; $g_{AB} = B_{BA} = g^{2^3} \cdot 3^3 \cdot 5^2$ *[6]*

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. lice 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 [8].*

Example 2 *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 $n! \gg 2n$.*

5. Supersingular isogeny Diffie–Hellman key exchange (SIDH)

This paragraph recalls the SIDH key exchange protocol . 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 her 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 Bob's 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 $j(E_{BA}) = j(E_{AB})$ [9].

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

Figure 6: *Comparison of Diffie-Hellman algorithms [10].*

6. Current isogeny problems

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 $\phi : E \to E/G$ [6].
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 [6].
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 [6].

Cryptography helps in building a more trusted world. When quantum computers appear, many modern methods of information protection will lose their validity and we will be forced to use newer and more reliable methods of information security.

References

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

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

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

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

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

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

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

[8] J. Siegel (2014) *Expander Graphs*

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

[10] C. Costello (2017) *An introduction to supersingular isogeny-based cryptography*. ECC 2017 Nijmegen https://ecc2017.cs.ru.nl/slides/ecc2017 school-costello.pdf