Isogeny-based cryptography

Table of content

1 Introduction

Post-quantum cryptography (PQC) is a young field anticipating the availability of large-scale quantum computers in the context of digital security. Seen by many as the next logical step to supersede classical computers, the quantum paradigm offers algorithms that could endanger classical public key cryptography. Possibly the most famous one, Shor's algorithm [] brings integer factorization down to a polynomial problem. This has obvious dire consequences for classical RSA and Diffie-Hellman (DH) protocols. The performances of current quantum computers are still far from reaching usability in attack scenarios. But cautiousness calls for quantum-resistant algorithms that could secure classical computers. In that regard, the NIST (National Institute of Standards of Technology) has organized competitions to foster developpment in PQC.

Different usages require different cryptosystems and as such there are multiple classes of post-quantum protocols investigated. Of interest in this paper is public-key cryptography (PKC) also known as asymmetric cryptography. The benefit of PKC stems from the fact that no pre-sharing of information is needed to establish a secure channel, hence making it very convinient. To achieve this, a Diffie-Hellman key-exchange protocol is usually used. In our case we use elliptic curve isogenies and associated hard homogeneous spaces (HHS) to build such a protocol.

More precisely, we investigate the Couveignes-Rostovtsev-Stolbunov protocol (CRS). This protocol works with isogenies bewteen ordinary curves with fixed complex multiplication over a finite field of prime order $\sim 2^{256}$. Key-exchanges using this scheme are comparatively slower than their supersingular counterpart such as SIDH protocols. However, CRS heuristically gives less room for potential attacks than SIDH. This is due to the fact that supersingular endomorphism rings embed as orders in quaternion algebras whereas ordinary ones embed in imaginary quadratic fields. As such, more structure is available for exploitation in an attack of SIDH protocols. This kind of structural attack has been demonstrated against the NTRU protocol and led to Prime-NTRU. Another advantage of CRS is that it is truely symmetric compared to SIDH where parties have to agree on specific primes to use.

The main focus of this project was to implement as efficiently as possible the CRS protocol following the 2018 article of Luca De Feo, Jean Kieffer and Benjamin Smith []. Recent publications on the subject of isogeny computation allow for very efficient walking algorithm in the isogeny graphs. On the one hand, *radical isogenies* [] are used to take k steps in the l-isogeny graph in time complexity $\mathcal{O}(k)$ for primes 3, 5 and 7. On the other hand, the $\sqrt{}$-*Velu* algorithm [] is used to take walk in the remaining graphs with time complexity $\mathcal{O}(k\sqrt{l})$. The reason this subject was choosen specifically is after a previous unoptimized JULIA implementation of these techniques. It gave promising results (around 35% faster than the 2018 implementation) but was neither optimized nor using the expected quadratic-twist symmetry. The second issue was completely resolved by our C implementation while drastic optimizations were found.

This paper is divided in three sections. The first one mainly accounts for the minimal mathematical background surrounding isogeny-graphs and complex multiplication. An exposition on the CRS protocol is also given. The second part tackles the architecture of the program. The complete project is around 4000 lines long. Its source code is available at []

along with a documentation. Finally, the third part reports prime-by-prime timing results, optimized bound for the secret keys as well as some inner data observed at runtime.

2 Theoretical background

In this section we introduce the necessary mathematical material surrounding the CRS protocol. It is assumed the reader has some familiarities with elliptic curves and their arithmetic. Still, we recall the fundamentals in order to underline some important aspect of the algorithms. We fix once and for all a prime number p. Unless indicated otherwise we assume throughout the section that curves are defined over $\mathbb{F}_p$, the field with p elements.

2.1 Elliptic curves and models

Recall the standard definition of an elliptic curve over k:

Definition. An elliptic curve E over a field k is a smooth curve given by a (dehomogenized) polynomial $F \in k[x, y]$ of the form

$$F = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6).$$

This presentation of the curve is usually called the *Weierstrass* form. It is said to be in *short Weierstrass* form if the coefficients a_1, a_2 and a_3 are null. The following proposition allow one to only consider short Weierstrass equations except for some fields.

Proposition. An elliptic curve E over a field k of caracteristic different from 2 and 3 is isomorphic to an elliptic curve in short Weierstrass form.

Proof. See Silverman III.1. [] □

The (short-)Weierstrass models admit explicit formulas that reflect the group law of the elliptic curve. It turns out that other models have better, faster properties when it comes to group operations. The following *Montgomery* model has one of the fastest doubling operation of all. It also has a fast scalar multiplication which we talk about in the next section.

Definition. A *Montgomery curve* or an elliptic curve in *Montgomery* form over a field k is an elliptic curve $E_{A,B}$ given by a polynomial $F \in k[x, y]$ of the form

$$F = By^2 - x(x^2 + Ax + 1)$$

with $A, B \in k$ satisfying $b \neq 0$ and $A^2 \neq 4$.

All Mongomery curves admit a short Weierstrass model via the variable change $x := x/B$ and $y := y/B$. The following proposition show which short Weierstrass curves admit a Montgomery model.

Proposition. The elliptic curve $y^2 = x^3 + ax + b$ over a field k admits a Montgomery model if

- The polynomial $X^3 + aX + b$ has a root w in k
- $3w^2 + a$ is a quadratic residue in k.

Proof. Under the above conditions, set $u = (3w^2 + a)^{-\frac{1}{2}}$. The (admissible) variable change $x := u(x - w)$, $y := uy$ show that the curve has Montgomery model $E_{A,B}$ with $A = 3wu$ and $B = u$. □

Associated to an elliptic curve E is the fundamental quantity called *j-invariant*. For a Mongomery curve $E_{A,B}$ over a field k of caracteristic different from 2 and 3 one has

$$j = \frac{256(A^3 - 3)^3}{A^2 - 4}.$$

Elliptic curves can be shown to be isomorphic if and only if they have the same j-invariant. The crucial thing to remember is that this classification only happens over the algebraic closure $\bar{k}$ of the base field k. Curves can be isomorphic over $\bar{k}$ while being non-isomorphic over k or a finite extension of k. In fact, the B parameter in the definition of a Mongomery curve account for two isomorphism classes: take $A, B, B' \in k$ and consider the curve $E_{A,B}$ and $E_{A,B'}$. One easily show that they are isomorphic at best over $k(\sqrt{B/B'})$. Hence they are isomorphic over k if and only if B/B' is a quadratic residue. We call $E_{A,B'}$ a *quadratic twist* of $E_{A,B}$.

The next and last model of elliptic curve is called the *Tate normal* form. It will be used when dealing with radical isogenies.

Definition. An Elliptic curve in *Tate normal* form over a field k is an elliptic curve E given by a polynomial $F \in k[x, y]$ of the form

$$F = y^2 + (1 - c)xy - by - x^2(x - b)$$

on which the point $(0, 0)$ has order at least 4. We also say E is in Tate normal form when given by

$$F = y^2 + (1 - c)xy - by - x^3$$

where $(0, 0)$ is of order 3.

The following lemma and its proof show how to transform a Mongomery curve along with a point P of order $N \geq 4$ into Tate normal form. We demonstrate the lemma with a general Weierstrass curve but only the Montgomery case with $B = 1$ interests us in the implementation. It is only a matter of setting some a-coefficients to 0 in the formulas.

Lemma 2.1.1. Let E be an elliptic curve over a field k and let $P = (x, y) \in E$ be a point of order $N \geq 3$. There exist a Tate normal model for E such that P is sent to $(0, 0)$..

Proof. We consider E in general Weierstrass form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

A translation from P to $(0, 0)$ allows us to remove a_6 and write the curve as

$$Y^2 + a_1XY + b_3Y = X^3 + b_2X^2 + b_4X.$$

where $b_2 = 3x + a_1$, $b_3 = 2y + a_1x + a_3$ and $b_4 = 3x^2 + 2a_1x + a_4$. The coefficient b_3 is non-zero as P does not have order 2. This can be read on the duplication formula. Let us remove the b_4 coefficient by the (admissible) change of variable $Y := Y + b_4/b_3X$. We get the representation

$$Y^2 + c_1XY + b_3Y = X^3 + c_2X^2.$$

where $c_1 = 2b_4/b_3 + a_1$ and $c_2 = b_2 - a_1b_4/b_3$.

Now introduce two free scaling variables $\alpha, \beta \in k$. The scaling $X = \alpha X$, $Y = \beta Y$ gives a model that is Tate normal if

$$\alpha^3 = \beta^2$$
$$\beta b_3 = c_2\alpha^2.$$

Following the standard negation formula and $N = 3$ being equivalent to $2P = -P$ we see that $c_2 = 0$ is also equivalent to $N = 3$. Assuming that $N \geq 4$, one find $\alpha = (b_3/c_2)^2$ and $\alpha = c_2/b_3$. Thus setting $b = -c_2(b_3/c_2)^2$ and $c = 1 - c_1(c_2/b_3)^2$ gives the Tate normal form. If $N = 3$, the curve is already in Tate normal form. □

Notice however that in the case $N = 3$, the coefficient b_3 should be computed to get b and c. This in turns involves knowing the value of y. As we will see with x-only arithmetic, over Mongomery curves it is better to use our free system in α and β. Setting $\alpha = b_3^3$ and $\beta = b_3^2$ we find a presentation which only involves y^2. In the end we find $b = -1/b_3^2$ and $c = 1 - 2b_4/b_3^2$. This will avoid us extracting a square root of $x^3 + ax^2 + 1$ to get a y value.