Francisco Rodríguez Henríquez

francisco@cs.cinvestav.mx

CINVESTAV-IPN
Computer Science Departament

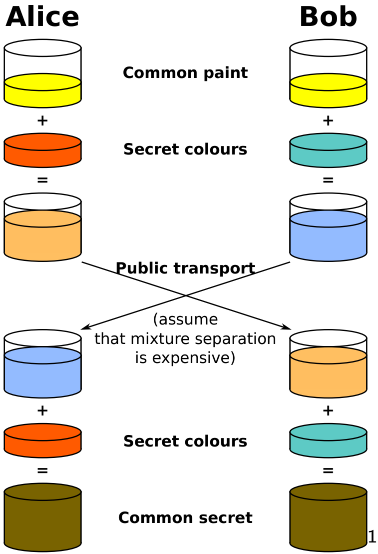
Friday 14th June, 2019

Table of contents

Secret Sharing - Diffie Hellman

Problem:

- Alice and Bob want to paint their houses using the same color.
- They just don't want Eve to know the final color.



[1]

[1] https://commons.wikimedia.org/wiki/File:Diffie-Hellman_Key_Exchange.svg

Discrete Log on finite fields

Public parameters

- Prime p,
- base g (generator).

Alice

Bob

Alice	Bob
Choose a random integer $a \in \{1, \ldots, p-1\}$.	Choose a random integer $b \in \{1, \ldots, p-1\}$.
Compute $g_a := g^a \mod p$.	Compute $g_b := g^b \mod p$.
Send g_a to Bob.	Send g_b to Alice.
Compute $g_{ba} := g_b^a \mod p$.	Compute $g_{ab} := g_a^b \mod p$.

$$g_{ab} = (g^a)^b = (g^b)^a = g_{ba}$$

Discrete log consists in find a knowing g and g_a.

Mathematical Background

An *Elliptic Curve* in Weierstrass short model over a finite field $\mathbb{F}_q$ where $q = p^m$ for some prime $p > 3$, is given by the equation

$$E/\mathbb{F}_q : Y^2 = X^3 + AX + B$$

where $A, B \in \mathbb{F}_q$. The *j-invariant* $j(E)$ of a curve acts like a "fingerprint" of a

curve and it is given by

$$j(E) = \frac{1728 \cdot 4A^2}{4A^2 + 27B^2}.$$

A point P in $E(\mathbb{F}_q)$ is a pair (x, y) such that $x^3 + Ax + B - y^2 = 0$. E is supersingular if

$$\#E(\mathbb{F}_q) = q + 1 + k \cdot p.$$

Cinvestav

Mathematical Background

- (Hasse's Theorem)The number of rational points in an elliptic curve is bounded by

$$\#E(\mathbb{F}_q) = q + 1 - t, \qquad | t | \leq 2\sqrt{q}.$$

- Let E be an elliptic curve and consider the integer t given by Hasse theorem. An elliptic curve is called *supersingular* if $p|t$ otherwise is called *ordinary*.

Mathematical Background

- We can **ADD** points
$$R := P + Q,$$
- **DBL** a point
$$[2]P := P + P$$
- and multiply by an integer
$$[m]P := P + P + \cdots + P, (m-1)(\text{times}).$$
- The minimum integer m shuch that $[m]P = \mathcal{O}$ is called the **order** of P.
- The **subgroup generated** by P is the set $\{P, [2]P, [3]P, \ldots, [m-1]P, \mathcal{O}\}$ and is denoted by $\langle P \rangle$.
- The m-**torsion subgroup** is defined as $E[m] = \{P \in E \mid [m]P = \mathcal{O}\}$.

- An *Isogeny* $\phi : E_0 \to E_1$ is an homomorphism between elliptic curves given by rational functions. Given P and Q in E_0 is fulfilled that
  - $\phi(P+Q) = \phi(P) + \phi(Q)$,
  - $\phi(\mathcal{O}) = \mathcal{O}$.
- The *Kernel* of an Isogeny ϕ is the set

$$K = \{P \in E \mid \phi(P) = \mathcal{O}\}.$$

- The degree of an isogeny is $s := \#K$
- If ϕ has degree s^e then we can "decompose" ϕ as the composition

$$\phi_{e-1} \circ \phi_{e-2} \circ \cdots \phi_1 \circ \phi_0$$

where ϕ_i has degree s.

Mathematical Background

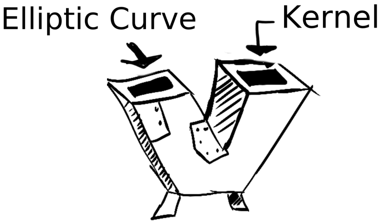
Theorem: Let E and E' be two elliptic curves. If there exists a degree-1 isogeny between E and E' then $j(E) = j(E')$. We say that E and E' are isomorphic. We denote that by $E \cong E'$.

Given an isogeny $\phi : E_0 \to E_1$ of degree d^e then

- We can "decompose" ϕ as the composition $\phi_{e-1} \circ \phi_{e-2} \circ \cdots \phi_1 \circ \phi_0$ where ϕ_i has degree d.
- There exists an isogeny $\hat{\phi} : E_1 \to E_0$ such that $\hat{\phi} \circ \phi = [d^e]$ and $\phi \circ \hat{\phi} = [d^e]$.

- Let E be an elliptic curve and $P \in E$ be an order m point.
- Then there exists an elliptic curve E_P and an isogeny $\phi_P : E \to E_P$ such that the *Kernel* of ϕ_P is $\langle P \rangle$, *i.e.* $\phi_P(p) = \mathcal{O}$ for each $p \in \langle P \rangle$. We write

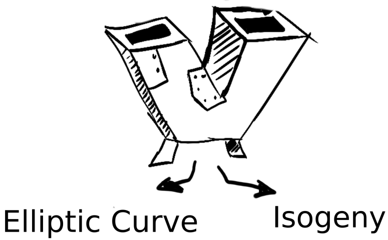
$$E_P = E/\langle P \rangle$$



Mathematical Background

- Let E be an elliptic curve and $P \in E$ be an order m point.
- Then there exists an elliptic curve E_P and an isogeny $\phi_P : E \to E_P$ such that the *Kernel* of ϕ_P is $\langle P \rangle$, *i.e.* $\phi_P(p) = \mathcal{O}$ for each $p \in \langle P \rangle$. We write

$$E_P = E/\langle P \rangle$$



State-of-the-art

SIDH Overview

- Luca De Feo, David Jao and Jérôme Plût proposed in 2014[FJP14] a new instance of Diffie-Hellman protocol using isogenies between supersingular elliptic curves as the core operation and curves as the secret shared (actually their j-invariants).
- They use a special kind of primes $p := \ell_a^{e_a} \ell_b^{e_b} f - 1$ which satisfies:
  - ℓ_a and ℓ_b are small primes,
  - $\log_2(\ell_a^{e_a}) \approx \log_2(\ell_b^{e_b})$,
  - f is a small integer which makes p to be a prime number.
- Public parameters are: prime p, an elliptic curve E_0, and points $P_a, Q_a, P_b, Q_b \in E_0$ such that $\langle P_a, Q_a \rangle = E[\ell_a^{e_a}]$ and $\langle P_b, Q_b \rangle = E[\ell_b^{e_b}]$.

Cinvestav

SIDH public parameters

$$\mathsf{p} := \quad 2^{e_2} \quad 3^{e_3} \quad f - 1$$

Such that $3^{e_3} \approx 2^{e_2}$

SIDH public parameters

Choose P_2 and Q_2
such that $\langle P_2, Q_2 \rangle = E[2^{e_2}]$

Choose P_3 and Q_3
such that $\langle P_3, Q_3 \rangle = E[3^{e_3}]$

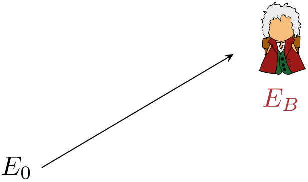
p := $2^{e_2} \quad 3^{e_3} \quad f - 1$

Such that $3^{e_3} \approx 2^{e_2}$

SIDH protocol

$K_B := P_2 + [n_2]Q_2$

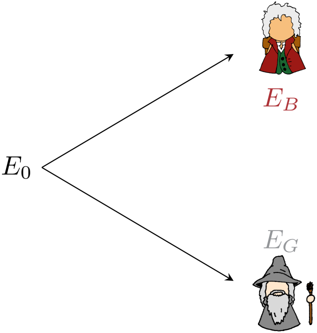
Get ϕ_B and $E_B = E_0/\langle K_B \rangle$



SIDH protocol

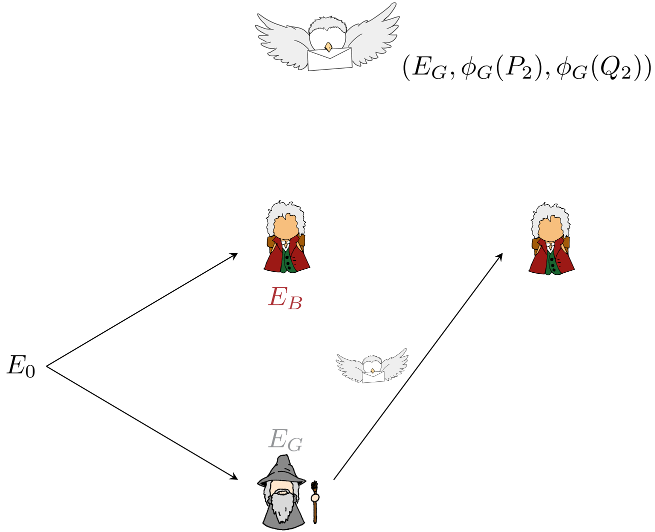
$$K_G := P_3 + [n_3]Q_3$$

Get ϕ_G and $E_G = E_0/K_G$



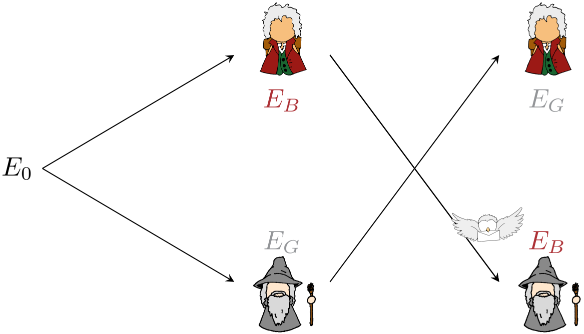
Cinvestav

SIDH protocol



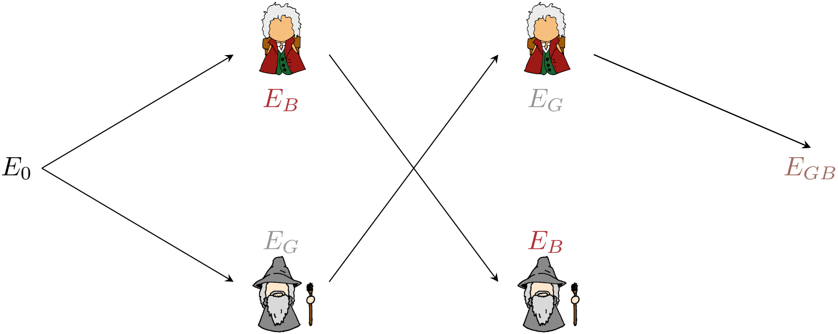
SIDH protocol

$(E_B, \phi_B(P_3), \phi_B(Q_3))$



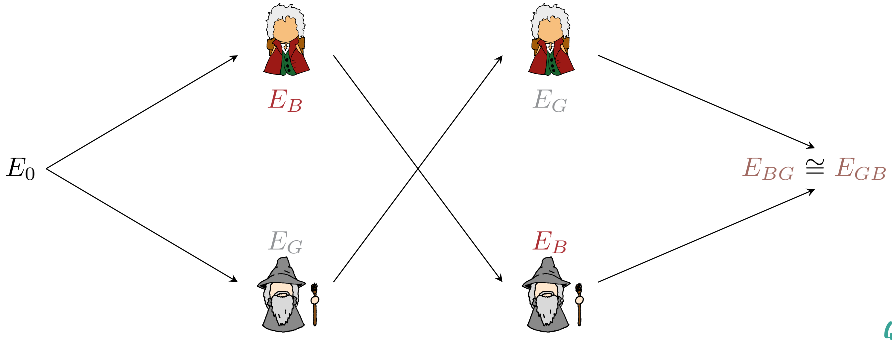
SIDH protocol

$$K'_B := \phi_G(P_2) + [n_2]\phi_G(Q_2)$$
Get $E_{GB} = E_G/\langle K'_B \rangle$



SIDH protocol

$$K'_G := \phi_B(P_3) + [n_3]\phi_B(Q_3))$$
Get $E_{BG} = E_B / \langle K'_G \rangle$



The Models

- There are different Models (equations) for elliptic curves.

Twisted Edwards Model

Twisted Edwards Curves:

$$E_{(a,d)}/\mathbb{F}_q : ax^2 + y^2 = 1 + dx^2y^2.$$

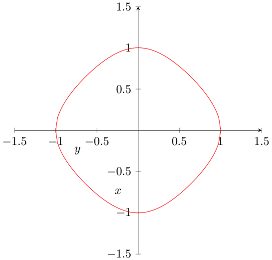
Advantages:

- Faster enough to be considered in some standards.
- Allows a y-only arithmetic.

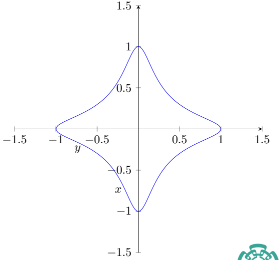
$$P = \left(\frac{x}{z}, \frac{y}{z}\right)$$

$$\mathcal{Y}(P) = (y_P : z_P)$$

- Complete addition formulas.
- Dustin Moody and Daniel Shumow[MS11] proposed formulas for computing isogenies between Twisted Edwards curves[2].



$x^2 + y^2 = 1 - x^2y^2$



$x^2 + y^2 = 1 - 30x^2y^2$

[2]Also for non-twisted Edwards curves and Huff curves

Montgomery Model

Projective Constant Montgomery Curves:

$$E_{(A:C)}/\mathbb{F}_q : Cy^2 = x(Cx^2 + Ax + C).$$

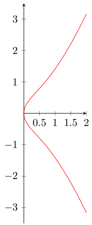
Advantages:

- Faster enough to be considered in some standards.
- Allows an x-only arithmetic.

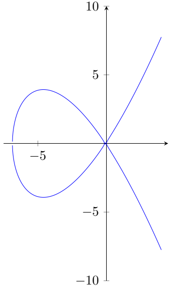
$$P = \left(\frac{x}{z}, \frac{y}{z}\right)$$

$$\mathcal{X}(P) = (x_P : z_P)$$

- Costello and Hisil [CH17] proposed formulas for computing isogenies between Montgomery curves.



$y^2 = x(x^2 + 1)$



$3y^2 = x(x^2 + 7x + 1)$

There and back again

We can transfer back and forth from Montgomery to Edwards curves "almost for free":

$$
\begin{aligned}
E_{(a,d)} &\to E_{(A:C)} \\
(y : z) &\mapsto (z + y : z - y), \\
(a, d) &\mapsto \left(\frac{a+d}{2} : \frac{a-d}{4}\right)
\end{aligned}
$$

$$
\begin{aligned}
E_{(A:C)} &\to E_{(a,d)} \\
(x : z) &\mapsto (x - z : x + z), \\
(A : C) &\mapsto (A + 2C, A - 2C)
\end{aligned}
$$

"How to get" an s-isogeny for $s = 2\ell + 1$.

Edwards	Montgomery
Order s point $K_e \in E_{a,d}$.	Order s point $K_m \in E_{(A:C)}$.
$E_{a,d} \xrightarrow{\phi} E_{a',d'}$	$E_A \xrightarrow{\phi} E_{A'}$
$a' := B_z a^s, \quad d' = B_y^8 d^s,$	$A' = (6\sigma + A) \cdot \pi^2$
$B_y = \prod_{i=1}^{\ell} y_{[i]K_e}.$	$\sigma_x = \sum_{i=1}^{\ell} \frac{z_{[i]K}^2 - x_{[i]K}^2}{x_{[i]K} z_{[i]K}}$
$B_z = \prod_{i=1}^{\ell} z_{[i]K_e}.$	$\pi_x = \prod_{i=1}^{\ell} x_{[i]K_m}, \pi_z = \prod_{i=1}^{\ell} z_{[i]K_m}.$

Cinvestav

Eval s-isogeny

Eval an s-isogeny for $s = 2\ell + 1$.

Edwards...

Eval s-isogeny

Eval an s-isogeny for $s = 2\ell + 1$.

It does not works in the sense that there is not an evaluation using only YZ-coordinates

Eval an s-isogeny for $s = 2\ell + 1$.

MontgomeryOrder s point $K_m \in E_{(A:C)}$.Point $Q \in E_{(A:C)}$ not in

$\langle K_m \rangle$.$\phi_{K_m}(\mathcal{X}(Q)) = (x_{Q'} : z_{Q'})$.$x_{Q'} =$

$$x_Q \cdot \left(\prod_{i=1}^{\ell} \left[(x_Q - z_Q)(x_{[i]K_m} + z_{[i]K_m}) + (x_Q + z_Q)(x_{[i]K_m} - z_{[i]K_m}) \right] \right)^2$$

$z_{Q'} =$

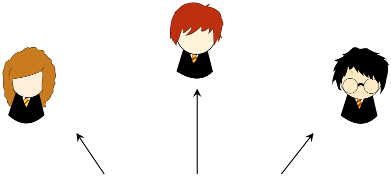
$$z_Q \cdot \left(\prod_{i=1}^{\ell} \left[(x_Q - z_Q)(x_{[i]K_m} + z_{[i]K_m}) - (x_Q + z_Q)(x_{[i]K_m} - z_{[i]K_m}) \right] \right)^2$$

Cost per iteration: 2**M** + 2**S**

Contribution

3. Extended SIDH
   - eSIDH
   - CRT + eSIDH
   - Parallelism in s^e-degree isogenies
4. Edwards-Montgomery Hybridization
   - There and back again
5. Results
   - Proposals
   - Results

Parameters



$$p := 2^{e_2}\ 3^{e_3}\ 5^{e_5}\ f - 1$$

Such that $3^{e_3}5^{e_5} \approx 2^{e_2}$
and $3^{e_3} \approx 5^{e_5}$

Parameters

Choose P_3 and Q_3
such that $\langle P_3, Q_3 \rangle = E[3^{e_3}]$

Choose P_2 and Q_2
such that $\langle P_2, Q_2 \rangle = E[2^{e_2}]$

Choose P_5 and Q_5
such that $\langle P_5, Q_5 \rangle = E[5^{e_5}]$

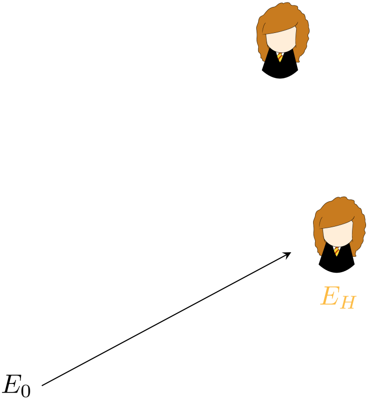
$$p := 2^{e_2} \quad 3^{e_3} \quad 5^{e_5} \quad f - 1$$

Such that $3^{e_3} 5^{e_5} \approx 2^{e_2}$
and $3^{e_3} \approx 5^{e_5}$

Define $S := P_3 + P_5$ and $T := Q_3 + Q_5$
to be the public parameters of Ron and Harry

eSIDH

$K_2 := P_2 + [n_2]Q_2$
Get ϕ_H and E_H

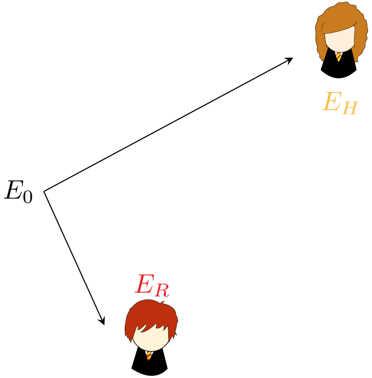


eSIDH

Parallel

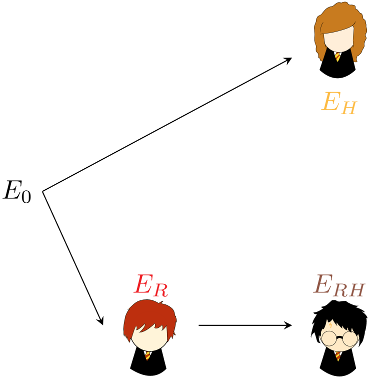
$K_3 := P_3 + [n_3]Q_3$ $\qquad$ $K_5 := P_5 + [n_5]Q_5$

Get ϕ_R and E_R. Send $\phi_R(K_5)$ to Harry.

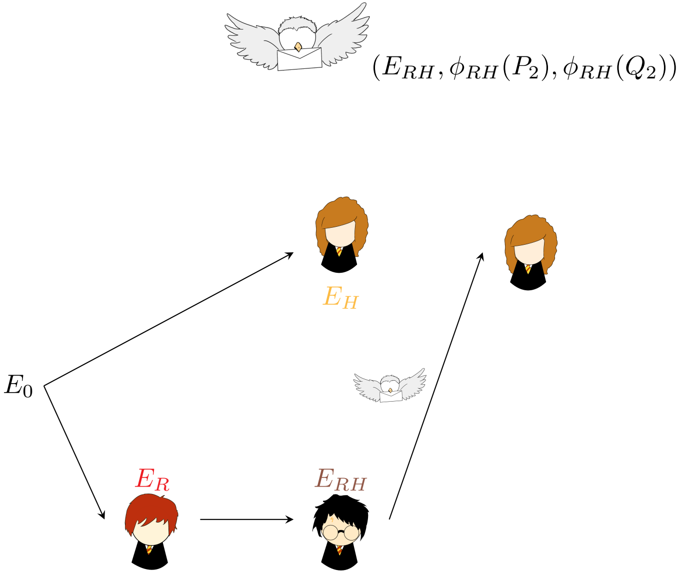


eSIDH

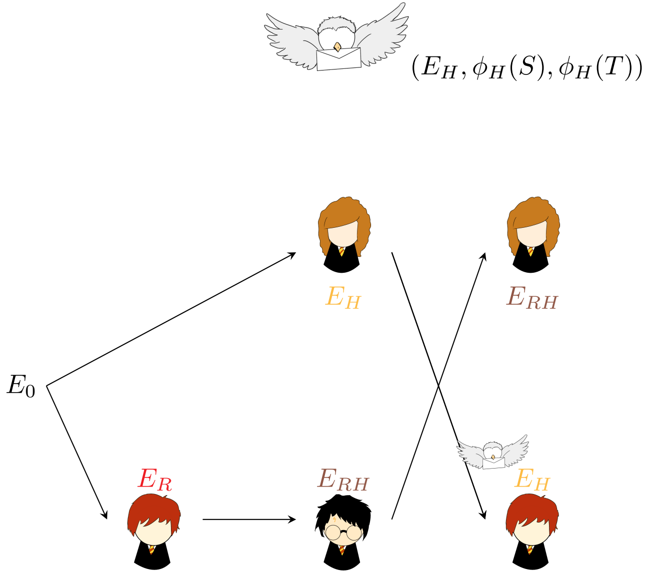
Use $\phi_R(K_5)$ to get E_{RH} and ϕ_{RH}



eSIDH

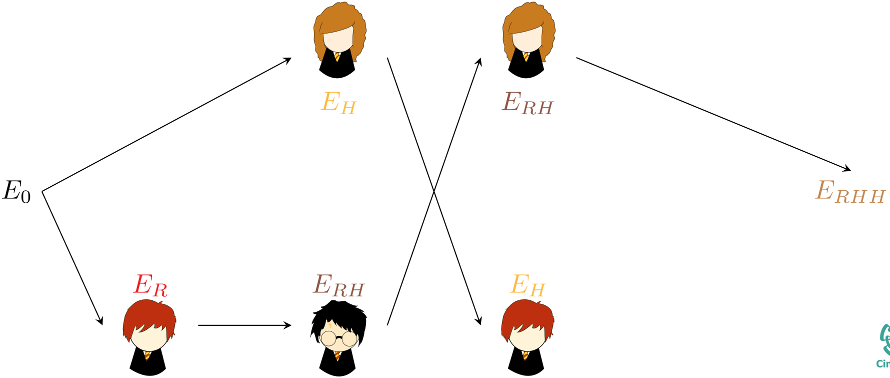


eSIDH



$$K_2' := \phi_{RH}(P_2) + [n_2]\phi_{RH}(Q_2)$$

Get E_{RHH}

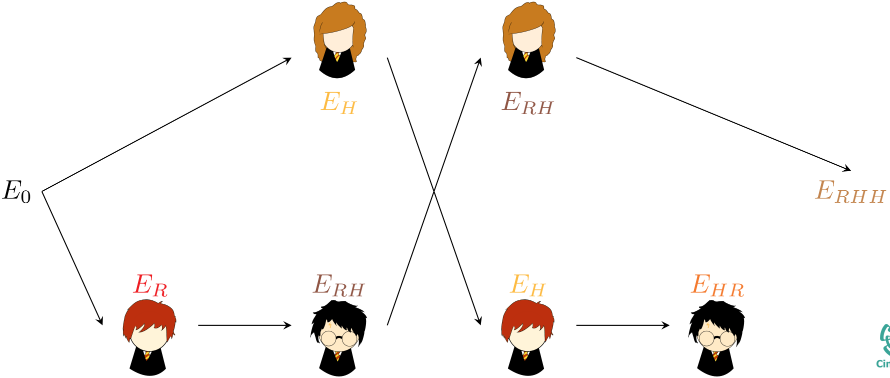


eSIDH

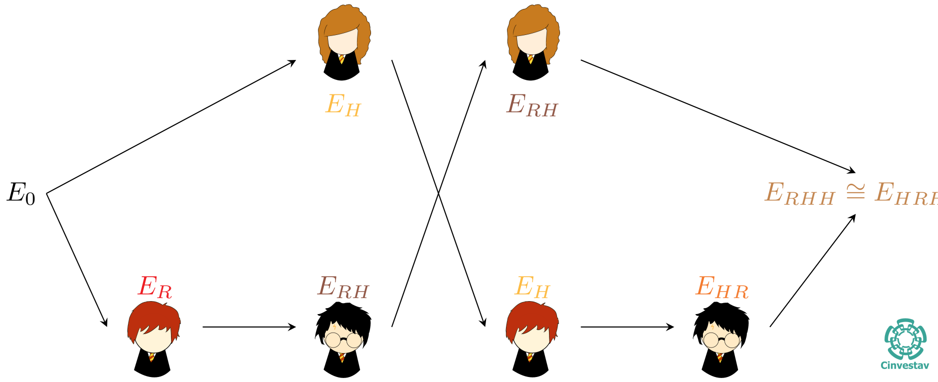
Parallel

$K'_3 := [5^{e_5}](\phi_H(S) + [n_3]\phi_H(T))$ $\quad$ $K'_5 := [3^{e_3}](\phi_H(S) + [n_5]\phi_H(T))$

Get ϕ'_R and E_{HR}. Send $\phi'_R(K'_5)$ to Harry.



Use $\phi'_R(K'_5)$ to get E_{HRH}



Cinvestav

CRT + eSIDH

- Choose $n_3 \in [1, 3^{e_3}]$ and $n_5 \in [1, 5^{e_5}]$ such that $(n_3, 5^{e_5}) = (n_5, 3^{e_3}) = 1$.
- Compute $\hat{n}_3 := n_3^{-1} \mod 5^{e_5}, \quad \hat{n}_5 := n_5^{-1} \mod 3^{e_3}$.
- Finally compute the integer private keys
  - $(\bar{n}_3 := n_3 \cdot \hat{n}_3 \mod 3^{e_3}, \ \bar{n}_5 := n_5 \cdot \hat{n}_5 \mod 5^{e_5})$.
  - $n_{35} := n_3 \cdot \hat{n}_3 \cdot n_5 \cdot \hat{n}_5 \mod (3^{e_3} 5^{e_5})$.

CRT + eSIDH

- Choose $n_3 \in [1, 3^{e_3}]$ and $n_5 \in [1, 5^{e_5}]$ such that $(n_3, 5^{e_5}) = (n_5, 3^{e_3}) = 1$.
- Compute $\hat{n}_3 := n_3^{-1} \mod 5^{e_5}, \quad \hat{n}_5 := n_5^{-1} \mod 3^{e_3}$.
- Finally compute the integer private keys
  - $(\bar{n}_3 := n_3 \cdot \hat{n}_3 \mod 3^{e_3},\ \bar{n}_5 := n_5 \cdot \hat{n}_5 \mod 5^{e_5})$.
  - $n_{35} := n_3 \cdot \hat{n}_3 \cdot n_5 \cdot \hat{n}_5 \mod (3^{e_3} 5^{e_5})$.

Key Generation is the same as in previous approach

1. Ron computes: $K_3 := P_3 + [\bar{n}_3]Q_3$,
2. Harry computes: $K_5 := P_5 + [\bar{n}_5]Q_5$.
3. Ron computes: E_R, ϕ_R using K_3.
4. Harry computes: E_{RH}, ϕ_{RH} using $\phi_R(K_5)$.

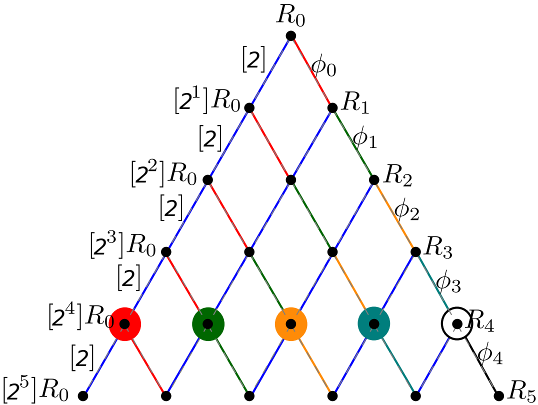
Cinvestav

CRT + eSIDH

- Choose $n_3 \in [1, 3^{e_3}]$ and $n_5 \in [1, 5^{e_5}]$ such that $(n_3, 5^{e_5}) = (n_5, 3^{e_3}) = 1$.
- Compute $\hat{n}_3 := n_3^{-1} \mod 5^{e_5}, \quad \hat{n}_5 := n_5^{-1} \mod 3^{e_3}$.
- Finally compute the integer private keys
  - $(\bar{n}_3 := n_3 \cdot \hat{n}_3 \mod 3^{e_3},\ \bar{n}_5 := n_5 \cdot \hat{n}_5 \mod 5^{e_5})$.
  - $n_{35} := n_3 \cdot \hat{n}_3 \cdot n_5 \cdot \hat{n}_5 \mod (3^{e_3} 5^{e_5})$.

Key agreement phase:

1. Ron computes: $K' := \phi_H(P_3) + [n_{35}]\phi_H(Q_3)$,
2. Ron computes: $K'_3 := [5^{e_5}]K'$.
3. Ron computes: E_{HR}, ϕ'_R using K_3.
4. Harry computes: E_{HRH}, ϕ'_{RH} using $\phi'_R(K')$.

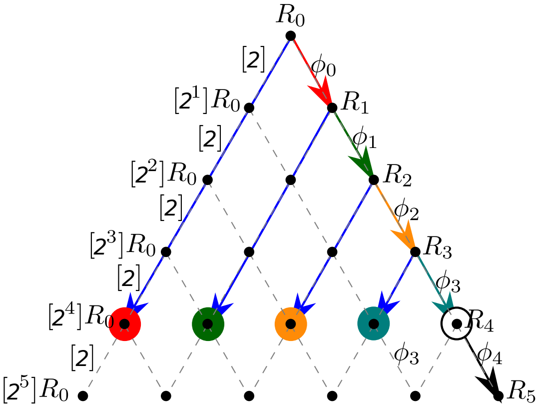


Example for a 2^5-isogeny.

Rules:

- Once you go down, you can't go back.
- The only way to go down along a non-blue line is reaching first the dot rounded by the same color of the line. Example: if you want to go down by a red line, first you need to reach the dot rounded by a red circle.

Parallelism in s^e-degree isogenies

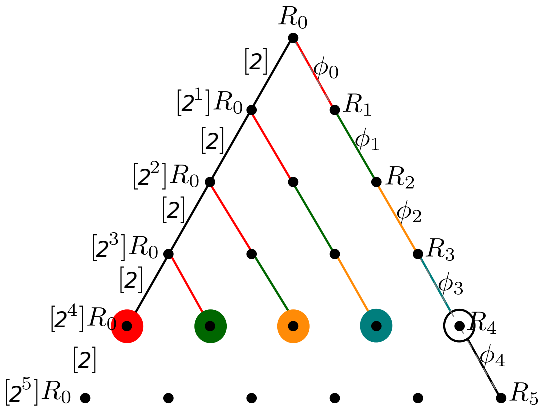


Example for a 2^5-isogeny.

Rules:

- Once you go down, you can't go back.
- The only way to go down along a non-blue line is reaching first the dot rounded by the same color of the line. Example: if you want to go down by a red line, first you need to reach the dot rounded by a red circle.

Parallelism in s^e-degree isogenies

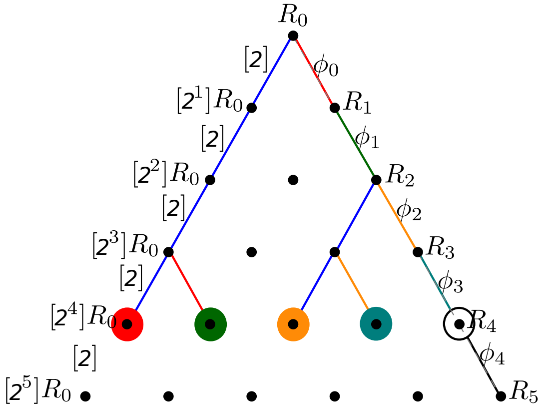


Unbalanced path: Evaluation oriented

Costs:

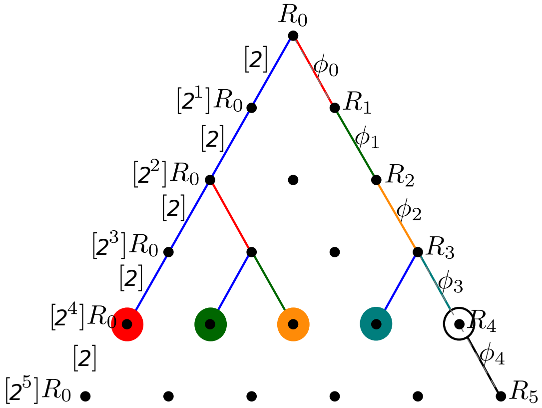
- $[2]$: 4
- Evaluations : 10

Fully parallelizable. (Need more than 250 cores in real life)



Balanced path
Costs:

- $[2]$: 6
- Evaluations : 6



Balanced path
Costs:

- [2] : 6
- Evaluations : 6

There and back again

- We make use of Edwards isogeny construction

There and back again

- We make use of Edwards isogeny construction
- Montgomery evaluation use Kernel points in YZ-Coordinates.

$$
\begin{aligned}
x' =& \mathbf{x_Q} \cdot \left(\prod_{i=1}^{\ell} \left[z_Q y_{[i]P} + y_Q z_{[i]P} \right] \right)^2 \\
z' =& \mathbf{z_Q} \cdot \left(\prod_{i=1}^{\ell} \left[z_Q y_{[i]P} - y_Q z_{[i]P} \right] \right)^2 .
\end{aligned}
$$

Cinvestav

There and back again

- We make use of Edwards isogeny construction
- Montgomery evaluation use Kernel points in YZ-Coordinates.
- Once that the Kernel points are in YZ-coordinates it is not necessary to go back to Montgomery anymore.

There and back again

- We make use of Edwards isogeny construction
- Montgomery evaluation use Kernel points in YZ-Coordinates.
- Once that the Kernel points are in YZ-coordinates it is not necessary to go back to Montgomery anymore.
- Translate `xDBL` and `xADD` into `yDBL` and `yADD` respectively to compute $[i]K$.

Proposals

Our proposals	[JAC+17] proposals
$P_{508} = 2^{258}3^{74}5^{57} - 1$	$P_{503} = 2^{250}3^{159} - 1$
$P_{764} = 2^{391}3^{121}5^{78} - 1$	$P_{751} = 2^{372}3^{239} - 1$
$P_{1013} = 2^{512}3^{157}5^{108} - 1$	$P_{964} = 2^{486}3^{301} - 1$
	[ACVCD+18] proposals
$P_{443} = 2^{222}3^{73}5^{45} - 1$	$P_{434} = 2^{216}3^{137} - 1$
$P_{557} = 2^{280}3^{86}5^{61} - 1$	$P_{546} = 2^{273}3^{172} - 1$

Table 1: Our proposals for eSIDH primes in comparison with the current state-of the art

Our proposals	[JAC+17] proposals
$P_{508} = 2^{258}3^{74}5^{57} - 1$	$P_{503} = 2^{250}3^{159} - 1$
$P_{764} = 2^{391}3^{121}5^{78} - 1$	$P_{751} = 2^{372}3^{239} - 1$
$P_{1013} = 2^{512}3^{157}5^{108} - 1$	$P_{964} = 2^{486}3^{301} - 1$
	[ACVCD+18] proposals
$P_{443} = 2^{222}3^{73}5^{45} - 1$	$P_{434} = 2^{216}3^{137} - 1$
$P_{557} = 2^{280}3^{86}5^{61} - 1$	$P_{546} = 2^{273}3^{172} - 1$

Table 1: Our proposals for eSIDH primes in comparison with the current state-of the art

- Our primes are Montgomery Friendly so we can achieve a faster modular reduction.
- There are more eSIDH primes than SIDH primes.
- It is possible to improve the security (few bits).

Implementation considerations

- We compare against the recent library version of Costello-Longa-Naehrig instead of the reported one [CLN16].
- We do not compare with results of Faz-López-Ochoa-Rodríguez article [FHLOJRH18] because the specifications submitted to NIST[JAC$^+$17] does not allow the use of all improvements reported by them.
- All the timings were measured using an Intel core i7-6700K processor with micro-architecture Skylake at 4.0 GHz. Using the Clang-3.9 compiler and the flags `-Ofast -fwrapv -fomit-frame-pointer -march=native -madx -mbmi2`.

Arithmetic Results

Operation	[JAC+17] p_{503}	**Ours** p_{509}	[JAC+17] p_{751}	**Ours** p_{765}	**Ours** p_{1013}
Mult $\mathbb{F}_{p^2}$	557	500	1,054	972	1,610
Sqr $\mathbb{F}_{p^2}$	411	370	769	711	1,217
Inv $\mathbb{F}_{p^2}$	110,927	102,530	314,354	250,131	675,623

Operation	[ACVCD+18] p_{434}	**Ours** p_{443}	[ACVCD+18] p_{546}	**Ours** p_{557}
Mult $\mathbb{F}_{p^2}$	509	467	774	680
Sqr $\mathbb{F}_{p^2}$	345	340	519	515
Inv $\mathbb{F}_{p^2}$	79,018	80,253	207,854	154,931

Table 2: Arithmetic cost comparison. Timings are reported in clock cycles measured over a Skylake processor at 4.0GHz.

Cinvestav

Protocol Results

	Alice KeyGen			Bob KeyGen			Alice KeyAgr			Bob KeyAgr		
	NP	**P**	**AF**	**NP**	**P**	**AF**	**NP**	**P**	**AF**	**NP**	**P**	**AF**
P503 [JAC+17]		8.24			9.13			6.70			7.71	
$2^{258} \cdot 3^{74} \cdot 5^{57} \cdot 1 - 1$	7.50	5.92	1.39	8.04	5.46	1.67	6.11	5.38	1.43	7.58	5.55	1.38
P751 [JAC+17]		23.72			26.70			19.38			22.81	
$2^{391} \cdot 3^{121} \cdot 5^{78} \cdot 1 - 1$	22.27	16.72	1.42	24.10	15.43	1.73	18.35	15.32	1.26	22.77	15.78	1.44
$2^{512} \cdot 3^{157} \cdot 5^{108} \cdot 1 - 1$	49.27	36.44		54.79	34.57		40.84	33.26		51.78	35.40	
P434 [ACVCD+18]		5.3			5.9			5.0			5.8	
$2^{222} \cdot 3^{73} \cdot 5^{45} \cdot 1 - 1$	5.93	4.68	1.13	6.60	4.61	1.28	4.79	4.27	1.17	6.17	4.69	1.23
P546 [ACVCD+18]		10.6			11.6			9.9			11.3	
$2^{280} \cdot 3^{86} \cdot 5^{61} \cdot 1 - 1$	11.17	8.63	1.23	12.45	8.29	1.40	9.09	7.83	1.26	11.65	8.48	1.33

Table 3: Performance comparison of the eSIDH against the proposed in [JAC+17] and [ACVCD+18]. The running time is reported in 10^6 clock cycles measured in an Intel Skylake proccessor at 4.0 GHz.Parallel version performance using 3 cores.

Results

Publications

Accepted:

- Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes and Francisco Rodríguez-Henríquez. *On the cost of computing isogenies between supersingular elliptic curves*. Selected Areas in Cryptology 2018(Conference).

Work in progress:

- Daniel Cervantes-Vázquez, Eduardo Ochoa-Jiménez and Francisco Rodríguez-Henríquez. *A parallel approach for SIDH*.
- Daniel Cervantes-Vázquez, Mathilde Chenu-de-La Morinerie, Luca de Feo, Jesús Chi-Domínguez, Francisco Rodríguez-Henríquez and Ben Smith. *Stronger and Faster Side-Channel Protections for CSIDH*. Submitted.

Future Work

- To implement different parallel strategies and analyze those strategies.
- To study other models to improve performance (Huff, Split/Twisted Normal Form).

Bibliography I

[ACVCD+18] Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes, and Francisco Rodríguez-Henríquez.
On the cost of computing isogenies between supersingular elliptic curves.
Cryptology ePrint Archive, Report 2018/313, 2018.
https://eprint.iacr.org/2018/313.

[CH17] Craig Costello and Huseyin Hisil.
A simple and compact algorithm for sidh with arbitrary degree isogenies.
Cryptology ePrint Archive, Report 2017/504, 2017.
https://eprint.iacr.org/2017/504.

[CLN16] Craig Costello, Patrick Longa, and Michael Naehrig.
Efficient algorithms for supersingular isogeny diffie-hellman.
In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 572–601, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

Cinvestav

Bibliography II

[FHLOJRH18] A. Faz-Hernández, J. López, E. Ochoa-Jiménez, and F. Rodríguez-Henríquez.
A faster software implementation of the supersingular isogeny diffie-hellman key exchange protocol.
IEEE Transactions on Computers, pages 1–1, 2018.

[FJP14] Luca De Feo, David Jao, and Jérôme Plût.
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.
J. Mathematical Cryptology, 8(3):209–247, 2014.

[JAC+17] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik.
Supersingular isogeny key encapsulation, 2017.
sike.org.

Bibliography III

[MS11] Dustin Moody and Daniel Shumow.
Analogues of velu's formulas for isogenies on alternate models of elliptic curves.
Cryptology ePrint Archive, Report 2011/430, 2011.
https://eprint.iacr.org/2011/430.

Cinvestav