Echange de clés sur les graphes d'isogénies de courbes supersingulières,

ou comment Alice et Bob se promènent sur les graphes.

Projet de programmation en C
Mathilde de Chenu-de La Morinerie

SIKE


SIKE
Don't Do It

Supersingular Isogeny Key Exchange

Supersingular Isogeny Key Exchange

$\longrightarrow$ Diffie-Hellman sur les graphes d'isogénies de courbes supersingulières

Plan

1 Graphes d'isogénies

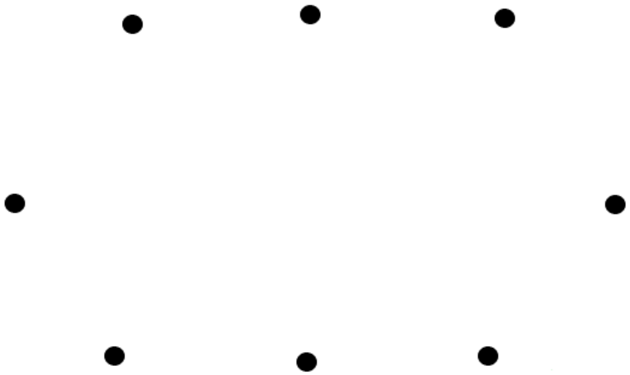
2 Promenade sur les graphes

3 Alice, Bob et Lisa

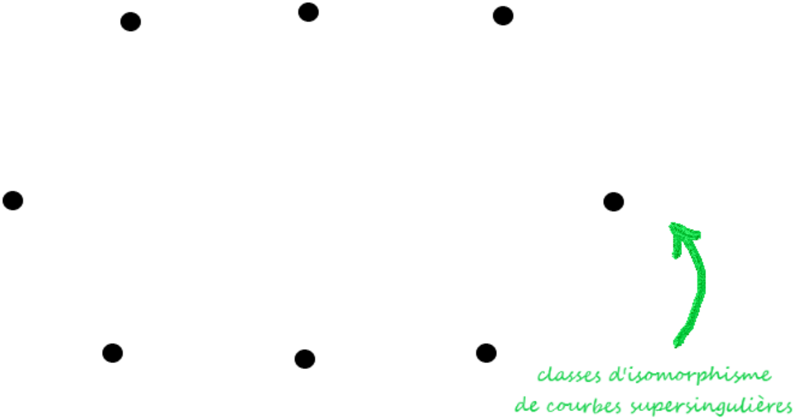
4 Généralisation

Graphes d'isogénies

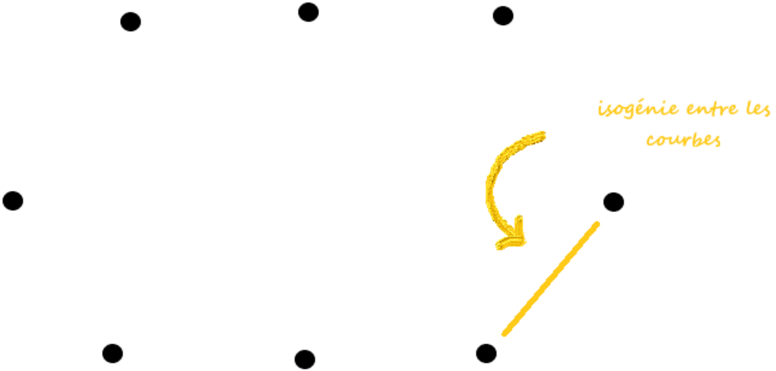
Points



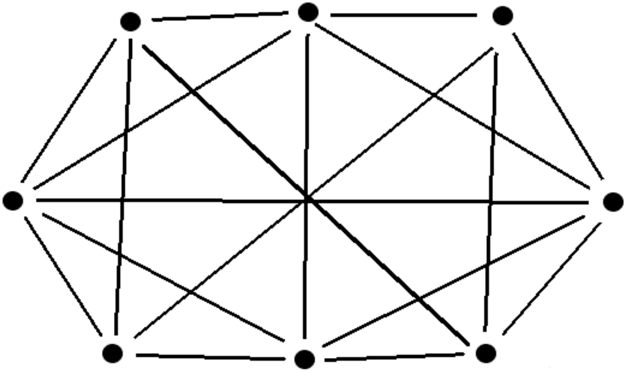
Graphes d'isogénies
Points



Graphes d'isogénies
Arêtes

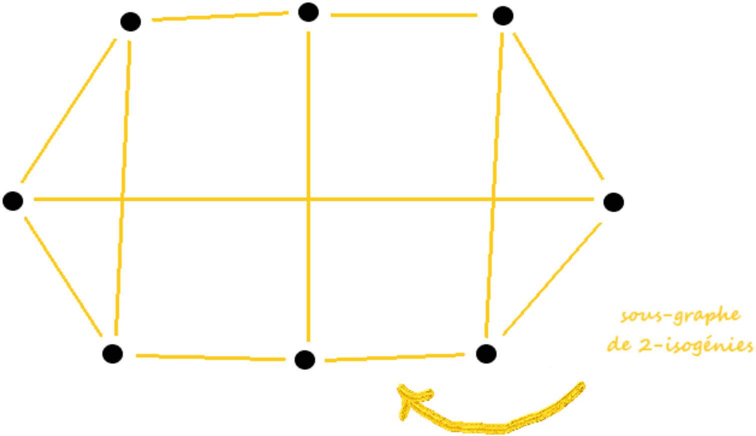


Graphes d'isogénies
Arêtes



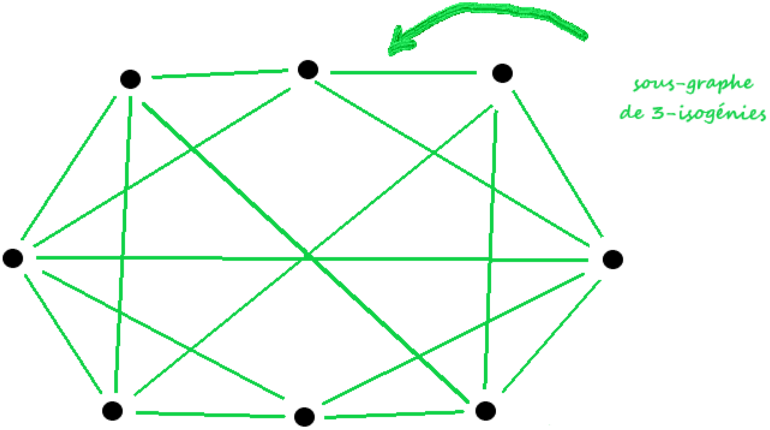
Graphes d'isogénies

2-isogénies

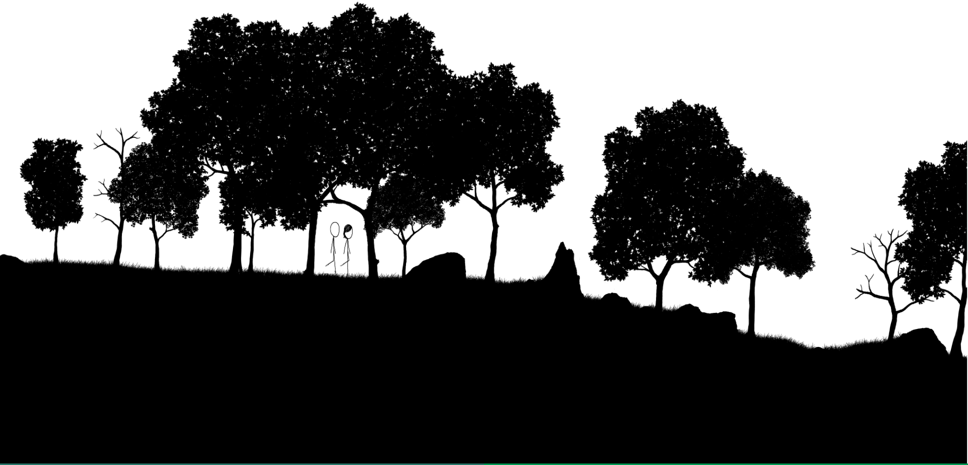


Graphes d'isogénies

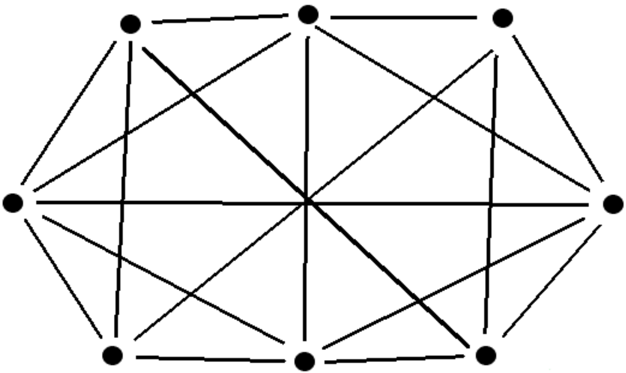
3-isogénies



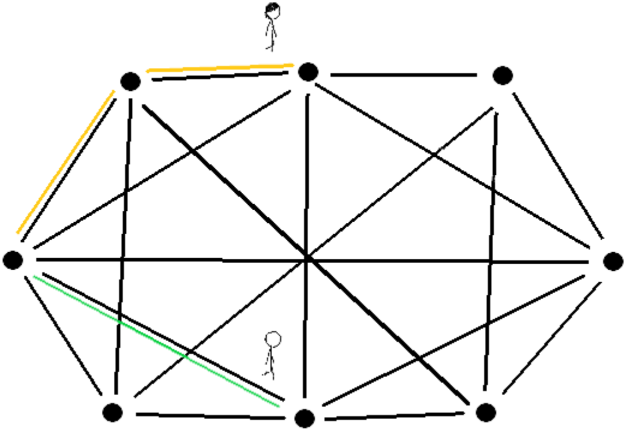
Alice et Bob se promènent dans la forêt...



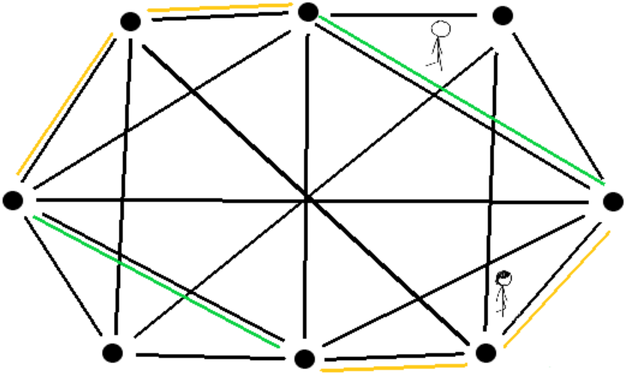
Alice et Bob se promènent dans la forêt...



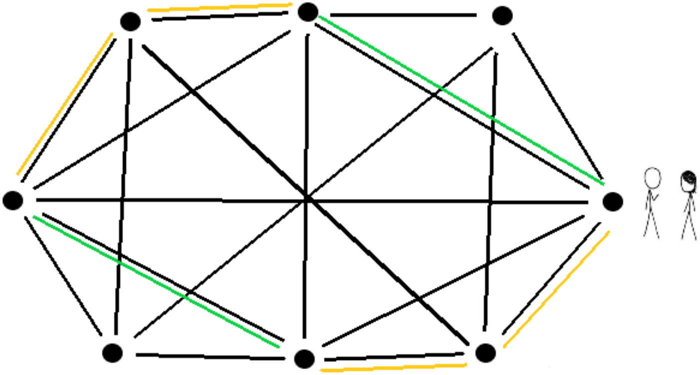
Alice et Bob décident de jouer à un jeu...



Alice et Bob décident de jouer à un jeu...



Alice et Bob décident de jouer à un jeu...



Alice et Bob interrogent Merlin

Alice et Bob interrogent Merlin

Il existe un
diagramme commutatif !

Diagramme commutatif

$$
\begin{tikzcd}
E \arrow[r, "\phi_a"] \arrow[d, "\phi_b"'] & E_a = E / < G_a > \arrow[d, "\phi_{ab}"'] \\
E_b = E / < G_b > \arrow[r, "\phi_{ba}"] & E_b / < \phi_b(G_a) > = E_a / < \phi_a(G_b) > = E_{ab}
\end{tikzcd}
$$

Diagramme commutatif

$$E \xrightarrow{\phi_a} E_a = {}^{E}/_{< G_a >}$$

Diagramme commutatif

$$\begin{tikzcd} E \arrow[r, "\phi_a"] \arrow[d, "\phi_b"'] & E_a = {}^{E}/_{< G_a >} \\ E_b = {}^{E}/_{< G_b >} & \end{tikzcd}$$

Diagramme commutatif

$$\begin{tikzcd}
E \arrow[r, "\phi_a"] \arrow[d, "\phi_b"'] & E_a = E / < G_a > \\
E_b = E / < G_b > \arrow[r, "\phi_{ba}"] & E_b / < \phi_b(G_a) >
\end{tikzcd}$$

Diagramme commutatif

$$\begin{tikzcd}
E \arrow[r, "\phi_a"] \arrow[d, "\phi_b"'] & E_a = E \big/ < G_a > \arrow[d, "\phi_{ab}"'] \\
E_b = E \big/ < G_b > \arrow[r, "\phi_{ba}"] & E_b \Big/ < \phi_b(G_a) > = E_a \Big/ < \phi_a(G_b) > = E_{ab}
\end{tikzcd}$$

Merlin fait du zèle

Trouver un chemin dans un graphe
d'isogénies supersingulières
est un problème difficile !

Alice et Bob décident de faire de la crypto

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2}3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2}3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2}3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2}3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

$\mathcal{A}$lice	$\mathcal{B}$ob
Clé secrète :	**Clé secrète :**
$m_a, n_a \in_R \mathbb{Z}/2^{e_2}\mathbb{Z}$	$m_b, n_b \in_R \mathbb{Z}/3^{e_3}\mathbb{Z}$

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2} 3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2} 3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

$\mathcal{A}$lice	$\mathcal{B}$ob
Clé secrète :	**Clé secrète :**
$m_a, n_a \in_R \mathbb{Z}/2^{e_2}\mathbb{Z}$	$m_b, n_b \in_R \mathbb{Z}/3^{e_3}\mathbb{Z}$
Clé publique :	**Clé publique :**
$E_a = E \Big/ < [m_a]P_a + [n_a]Q_a >$	$E_b = E \Big/ < [m_b]P_b + [n_b]Q_b >$
$\phi_a(P_b), \phi_a(Q_b)$	$\phi_b(P_a), \phi_b(Q_a)$

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2}3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2}3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

$\mathcal{A}$lice		$\mathcal{B}$ob
Clé secrète :		**Clé secrète :**
$m_a, n_a \in_R \mathbb{Z}/2^{e_2}\mathbb{Z}$		$m_b, n_b \in_R \mathbb{Z}/3^{e_3}\mathbb{Z}$
Clé publique :		**Clé publique :**
$E_a = E \big/ < [m_a]P_a + [n_a]Q_a >$		$E_b = E \big/ < [m_b]P_b + [n_b]Q_b >$
$\phi_a(P_b), \phi_a(Q_b)$		$\phi_b(P_a), \phi_b(Q_a)$
	$\overset{E_a, \phi_a(P_b), \phi_a(Q_b)}{\rightleftharpoons}$	
	$E_b, \phi_b(P_a), \phi_b(Q_a)$	

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2}3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2}3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

Alice		Bob
Clé secrète :		**Clé secrète :**
$m_a, n_a \in_R \mathbb{Z}/2^{e_2}\mathbb{Z}$		$m_b, n_b \in_R \mathbb{Z}/3^{e_3}\mathbb{Z}$
Clé publique :		**Clé publique :**
$E_a = E \Big/ < [m_a]P_a + [n_a]Q_a >$		$E_b = E \Big/ < [m_b]P_b + [n_b]Q_b >$
$\phi_a(P_b), \phi_a(Q_b)$		$\phi_b(P_a), \phi_b(Q_a)$
	$\xrightarrow{E_a, \phi_a(P_b), \phi_a(Q_b)}$	
	$\xleftarrow[E_b, \phi_b(P_a), \phi_b(Q_a)]{}$	
Calcul du secret :		**Calcul du secret :**
$G_{ab} = [m_a]\phi_b(P_a) + [n_a]\phi_b(Q_a)$		$G_{ba} = [m_b]\phi_a(P_b) + [n_b]\phi_a(Q_b)$
$E_{ab} = E_b \Big/ < G_{ab} >$		$E_{ba} = E_a \Big/ < G_{ba} >$

Alice et Bob décident de faire de la crypto

Paramètres publiques : $p = f \cdot 2^{e_2}3^{e_3} \pm 1$,
E supersingulière de cardinal $(p \pm 1)^2 = (f \cdot 2^{e_2}3^{e_3})^2$,
(P_a, Q_a) et (P_b, Q_b) bases respectives de $E[2^{e_2}]$ et $E[3^{e_3}]$.

$\mathcal{A}$lice		$\mathcal{B}$ob
Clé secrète :		**Clé secrète :**
$m_a, n_a \in_R \mathbb{Z}/2^{e_2}\mathbb{Z}$		$m_b, n_b \in_R \mathbb{Z}/3^{e_3}\mathbb{Z}$
Clé publique :		**Clé publique :**
$E_a = E \big/ < [m_a]P_a + [n_a]Q_a >$		$E_b = E \big/ < [m_b]P_b + [n_b]Q_b >$
$\phi_a(P_b), \phi_a(Q_b)$		$\phi_b(P_a), \phi_b(Q_a)$
	$\xrightarrow{E_a, \phi_a(P_b), \phi_a(Q_b)}$	
	$\xleftarrow[E_b, \phi_b(P_a), \phi_b(Q_a)]{}$	
Calcul du secret :		**Calcul du secret :**
$G_{ab} = [m_a]\phi_b(P_a) + [n_a]\phi_b(Q_a)$		$G_{ba} = [m_b]\phi_a(P_b) + [n_b]\phi_a(Q_b)$
$E_{ab} = E_b \big/ < G_{ab} >$		$E_{ba} = E_a \big/ < G_{ba} >$
Secret commun :		**Secret commun :**
$j(E_{ab})$		$j(E_{ba})$

Pourquoi ça marche ?

Pourquoi ça marche ?

- Choix des paramètres

Pourquoi ça marche ?

- Choix des paramètres

- Diagramme commutatif

Pourquoi ça marche ?

- Choix des paramètres

- Diagramme commutatif

- Sécurité

Lisa décide d'implémenter SIKE

Lisa décide d'implémenter SIKE

- Représenter efficacement les objets mathématiques

Lisa décide d'implémenter SIKE

- Représenter efficacement les objets mathématiques
  - Plus compact

Lisa décide d'implémenter SIKE

- Représenter efficacement les objets mathématiques
  - Plus compact
  - Plus rapide

Lisa décide d'implémenter SIKE

- Représenter efficacement les objets mathématiques
  - Plus compact
  - Plus rapide
- Calculer des isogénies

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a >$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > =< [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

- Couples de points $(P_a, Q_a), (P_b, Q_b)$:

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > =< [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
  $(P, Q) = (x_P, x_Q, x_{P-Q})$

Représenter les objets mathématiques
Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > =< [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
  $(P, Q) = (x_P, x_Q, x_{P-Q})$
- Courbe E :

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > =< [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
  $(P, Q) = (x_P, x_Q, x_{P-Q})$
- Courbe E : Courbes de Montgomery.

Représenter les objets mathématiques
Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$
$(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
$(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
$(P, Q) = (x_P, x_Q, x_{P-Q})$
- Courbe E : Courbes de Montgomery.
$by^2 = x^3 + ax^2 + x$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > =< [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
  $(P, Q) = (x_P, x_Q, x_{P-Q})$
- Courbe E : Courbes de Montgomery.
  $by^2 = x^3 + ax^2 + x \ \longrightarrow a$

Représenter les objets mathématiques

Plus compact

- Secret : $< [m_a]P_a + [n_a]Q_a > = < [m_a n_a^{-1}]P_a + Q_a >$
  $(m_a, n_a) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_a = m_a n_a^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$
  $(m_b, n_b) \in (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \longrightarrow s_b = m_b n_b^{-1} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$

- Couples de points $(P_a, Q_a), (P_b, Q_b)$:
  Ligne de Kummer : $(x_P, y_P) \longrightarrow x_P$
  $(P, Q) = (x_P, x_Q, x_{P-Q})$

- Courbe E : Courbes de Montgomery.
  $by^2 = x^3 + ax^2 + x \quad \longrightarrow a$
  Pas besoin de la courbe.

Représenter les objets mathématiques

Retrouver la courbe

$$a = \frac{(1 - x_p x_Q - x_P x_{P-Q} - x_Q x_{P-Q})^2}{4 x_P x_Q x_{Q-P}} - x_P - x_Q - x_{P-Q}$$

Représenter les objets mathématiques

Plus compact

$$p$$
$$E$$

$$P_a = (x_{P_a}, y_{P_a})$$
$$Q_a = (x_{Q_a}, y_{Q_a})$$

$$E_a = (a_1, a_2, a_3, a_4, a_5, a_6)$$
$$\phi_a(P_b) = (x_{\phi_a(P_b)}, y_{\phi_a(P_b)})$$
$$\phi_a(Q_b) = (x_{\phi_a(Q_b)}, y_{\phi_a(Q_b)})$$

Représenter les objets mathématiques

Plus compact

p E	p
$P_a = (x_{P_a}, y_{P_a})$ $Q_a = (x_{Q_a}, y_{Q_a})$	$x_{P_a}, x_{Q_a}, x_{P_a - Q_a}$
$E_a = (a_1, a_2, a_3, a_4, a_5, a_6)$ $\phi_a(P_b) = (x_{\phi_a(P_b)}, y_{\phi_a(P_b)})$ $\phi_a(Q_b) = (x_{\phi_a(Q_b)}, y_{\phi_a(Q_b)})$	$x_{\phi_a(P_b)}, x_{\phi_a(Q_b)}, x_{\phi_a(P_b - Q_b)}$

Représenter les objets mathématiques

Plus rapide

Représenter les objets mathématiques

Plus rapide

- Courbes de Montgomery :

Représenter les objets mathématiques

Plus rapide

- Courbes de Montgomery :
  Addition différentielle et échelles de Montgomery

Représenter les objets mathématiques

Plus rapide

- Courbes de Montgomery :
  Addition différentielle et échelles de Montgomery

- Éviter les inversions

Représenter les objets mathématiques

Plus rapide

- Courbes de Montgomery :
  Addition différentielle et échelles de Montgomery

- Éviter les inversions
  $x_P \longrightarrow (X_P : Z_P)$, $a \longrightarrow (A : C)$

Représenter les objets mathématiques
Plus rapide

- Courbes de Montgomery :
  Addition différentielle et échelles de Montgomery
- Éviter les inversions
  $x_P \longrightarrow (X_P : Z_P)$, $a \longrightarrow (A : C)$
- Éviter les calculs de racines

Représenter les objets mathématiques

Concrètement

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2 + 1)$

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$

Représenter les objets mathématiques
Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

- Points :

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

- Points :
  $(X : Z)$ ou $x = X/Z$

Représenter les objets mathématiques
Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

- Points :
  $(X : Z)$ ou $x = X/Z$
  structure de deux champs de $\mathbb{F}_{p^2}$.

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

- Points :
  $(X : Z)$ ou $x = X/Z$
  structure de deux champs de $\mathbb{F}_{p^2}$.

- Courbes :

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.

- Points :
  $(X : Z)$ ou $x = X/Z$
  structure de deux champs de $\mathbb{F}_{p^2}$.

- Courbes :
  $(A : C)$ ou $a = A/C$

Représenter les objets mathématiques

Concrètement

- Éléments de $\mathbb{F}_{p^2} \simeq \mathbb{F}_p[X] \Big/ (X^2+1)$
  $\longrightarrow x \in \mathbb{F}_{p^2}, x = s_0 + is_1$
  structure de deux champs gmp.
- Points :
  $(X : Z)$ ou $x = X/Z$
  structure de deux champs de $\mathbb{F}_{p^2}$.
- Courbes :
  $(A : C)$ ou $a = A/C$
  ou d'autres formats $((A-2C : 4C), (A+2C : A-2C)...)$

Calculer les isogénies

Calculer les isogénies

Théorème (Couveignes 06)

Toute isogénie est décomposable en une composition d'isogénies de degré premier.

Calculer les isogénies

Théorème (Couveignes 06)

Toute isogénie est décomposable en une composition d'isogénies de degré premier.

Calculer les 3^{e_3}-isogénies comme une suite de longueur e_3 de 3-isogénies successives.

Calculer les isogénies

Cas des 3-isogénies

Courbe image $(A' : C')$ par une isogénie de noyau $< P_3 > = < (X_3 : Z_3) >$:

$$(A' - 2C' : 4C') = \left((X_3 + Z_3)(Z_3 - 3X_3)^3 : 16X_3Z_3\right)$$

Point $(X' : Z')$ image de $(X : Z)$ par une isogénie de noyau $< P_3 > = < (X_3 : Z_3) >$:

$$(X' : Z') = \left(X(X_3X - Z_3Z)^2 : Z(Z_3X - X_3Z)^2\right)$$

Calculer les isogénies

Calculer les isogénies

G_b d'ordre 3^{e_3} sur E_0.

Calculer les isogénies

G_b d'ordre 3^{e_3} sur E_0.
$[3^{e_3-1}]G_b$ d'ordre 3 sur E_0.

Calculer les isogénies

G_b d'ordre 3^{e_3} sur E_0.
$[3^{e_3-1}]G_b$ d'ordre 3 sur E_0.
$E_1 = E_0 / < [3^{e_3-1}]G_b >$ est l'image de E_0 par la 3-isogénie de noyau $[3^{e_3-1}]G_b$.

Calculer les isogénies

Et ensuite ?

Calculer les isogénies

Et ensuite ?

$G_b^1 = \phi_1(G_b)$ d'ordre 3^{e_3-1} sur E_1.

Calculer les isogénies

Et ensuite ?

$G_b^1 = \phi_1(G_b)$ d'ordre $3^{e_3 - 1}$ sur E_1.
$[3^{e_3 - 2}]G_b^1$ d'ordre 3 sur E_1.

Calculer les isogénies

Et ensuite ?

$G_b^1 = \phi_1(G_b)$ d'ordre 3^{e_3-1} sur E_1.
$[3^{e_3-2}]G_b^1$ d'ordre 3 sur E_1.
$E_2 = E_1 \big/ < [3^{e_3-2}]G_b^1 >$ est l'image de E_1 par la 3-isogénie de noyau $[3^{e_3-2}]G_b^1$.

Calculer les isogénies

Et ensuite ?

Calculer les isogénies
Et ensuite ?

Et on recommence.

Calculer les isogénies

Et ensuite ?

Et on recommence.

On emmène en plus les points auxiliaires à chaque étape.

Calculer les isogénies

Cas des 2-isogénies

Calculer les isogénies
Cas des 2-isogénies

Même principe, mais avec les points de 4 torsion.

Calculer les isogénies
Cas des 2-isogénies

Même principe, mais avec les points de 4 torsion.

$$(A' - 2C' : 4C') = (X_4^4 - Z_4^4 : Z_4^4)$$

Calculer les isogénies
Cas des 2-isogénies

Même principe, mais avec les points de 4 torsion.

$$(A' - 2C' : 4C') = (X_4^4 - Z_4^4 : Z_4^4)$$

$$\begin{aligned}(X' : Z') = &(X(2X_4Z_4Z - (X_4^2 + Z_4^2)X)(X_4X - Z_4Z)^2 : \\ &Z(2X_4Z_4X - (X_4^2 + Z_4^2)Z)(Z_4X - X_4Z)^2)\end{aligned}$$


STAND BACK
I'M GOING TO TRY
SCIENCE

Calculer les isogénies

Cas général - Costello, Hisil 2017

Calculer les isogénies

Cas général - Costello, Hisil 2017

$$(X' : Z') = \left(X \prod_{i=1}^{d} \left(\frac{X \cdot X_{[i]P} - 1}{X - X_{[i]P}} \right)^2 : 1 \right)$$

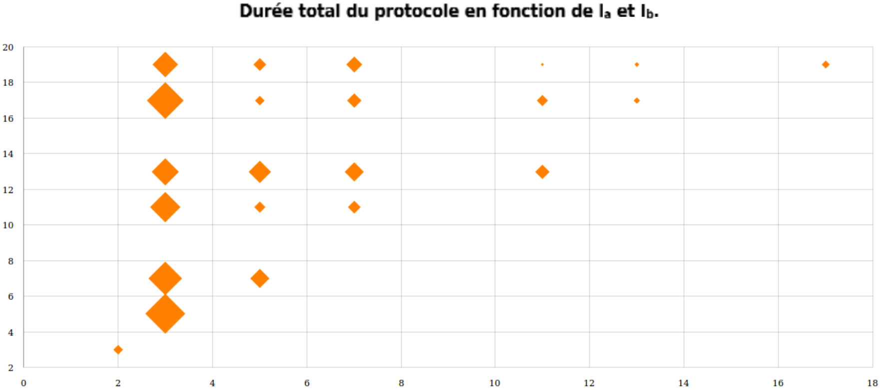
Calculer les isogénies

Cas général - Costello, Hisil 2017

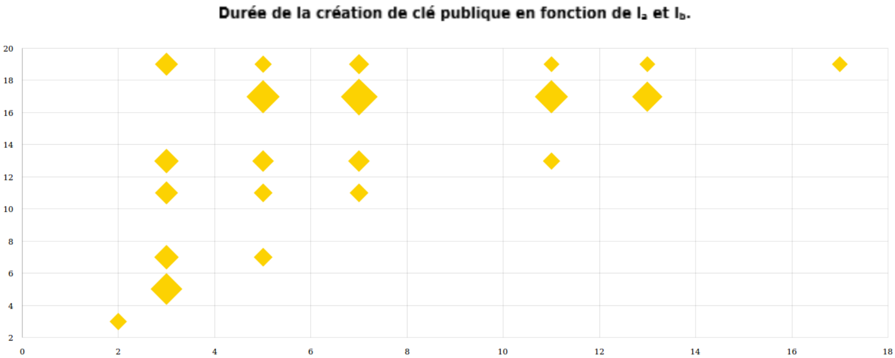
$$(X' : Z') = \left(X \prod_{i=1}^{d} \left(\frac{X \cdot X_{[i]P} - 1}{X - X_{[i]P}} \right)^2 : 1 \right)$$

$$(A' : C') = (X_2^2 + Z_2^2 : -X_2^2 Z_2^2)$$

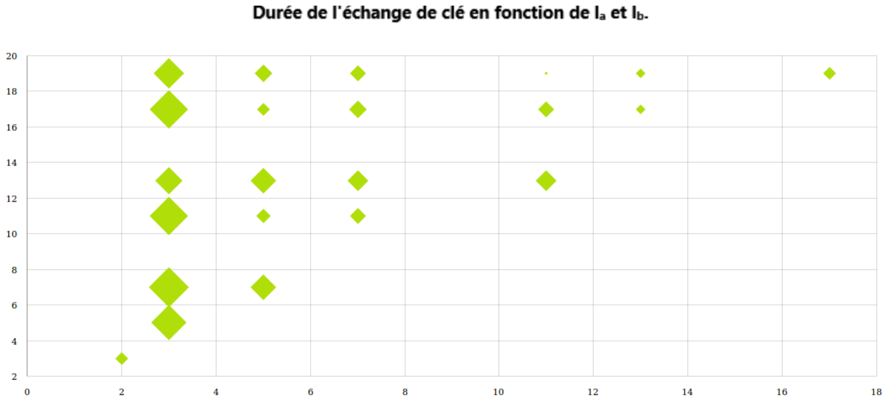
Comparaison des performances



Comparaison des performances



Comparaison des performances



Conclusion

Références

Spécification SIKE.
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, David Urbanik.
https ://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
2017.

A simple and compact algorithm for SIDH with arbitrary degree isogenies.
Craig Costello, Huseyin Hisil.
International Conference on the Theory and Application of Cryptology and Information Security. 2017.

Merci ! Des questions ?

$$E_0 \xrightarrow{\phi_1} E_0 \Big/ [\ell^{e-1}]S \xrightarrow{\phi_2} \dots \xrightarrow{\phi_i} E_{i-1} \Big/ [\ell^{e-i}]\phi_i(S) \xrightarrow{\phi_{i+1}} \dots \xrightarrow{\phi_e}$$
$$E_{e_1} \Big/ [\ell]\phi_{e-1}(S) = E_0 / < S >$$

Durées de la création de clé (k.g.), de l'échange de clé (k.e.) et de l'ensemble du protocole en fonction de

Les résultats sont exprimés en secondes.

	3			5			7			11			13			17			19		
	k.g.	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*	*k.g.*	*k.e.*	*tot.*
2	0.4	0.18	0.76																		
3				0.74	0.29	1.31	0.58	0.31	1.19	0.54	0.3	1.13	0.59	0.25	1.09	0.65	0.3	1.24	0.53	0.26	1.05
5							0.46	0.24	0.94	0.43	0.19	0.81	0.52	0.24	1	0.42	0.18	0.78	0.41	0.21	0.82
7										0.44	0.2	0.83	0.51	0.22	0.95	0.46	0.21	0.87	0.49	0.2	0.88
11													0.41	0.22	0.85	0.41	0.2	0.8	0.38	0.14	0.66
13																0.37	0.17	0.71	0.36	0.17	0.7
17																			0.39	0.18	0.74
19																					