Criptografia basada en isogènies

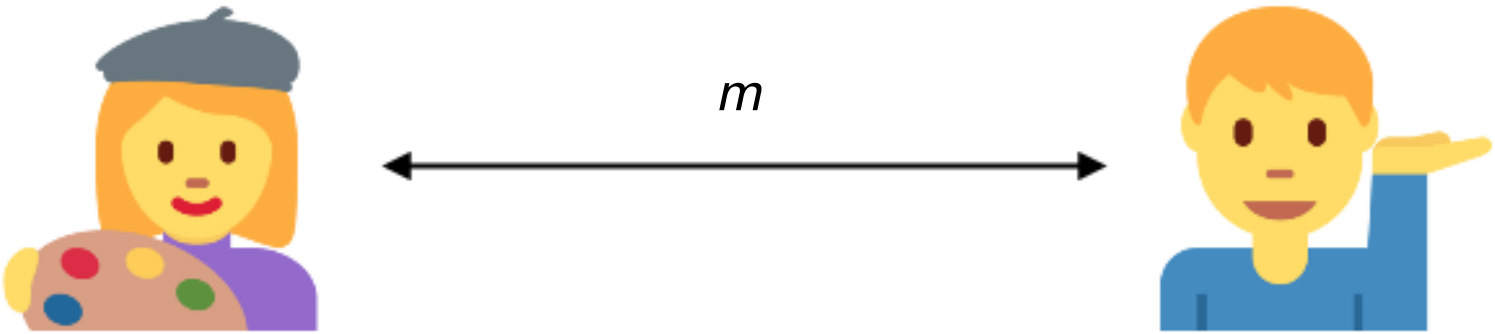
Enric Florit Zacarías

Directors: Xavier Guitart, Santiago Seguí i Ramsès Fernàndez

Departament de Matemàtiques i Informàtica – Universitat de Barcelona
Departament d'ITSecurity – Fundació Eurecat

7 de febrer de 2020

Introducció



Introducció

Alice

m

Bob

Eve

Introducció

Alice

xifrar(m, k)

Bob

Eve

Introducció

Alice

xifrar(m, k)

Estàndard: AES

Bob

Eve

Introducció

Alice

xifrar(m, k)

Estàndard: AES

Bob

Eve

Problema: com establir la clau k?

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3$$

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3 \xrightarrow{\cdot 3} 2$$

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3 \xrightarrow{\cdot 3} 2 \xrightarrow{\cdot 3} 6$$

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3 \xrightarrow{\cdot 3} 2 \xrightarrow{\cdot 3} 6 \xrightarrow{\cdot 3} 4$$

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3 \xrightarrow{\cdot 3} 2 \xrightarrow{\cdot 3} 6 \xrightarrow{\cdot 3} 4 \xrightarrow{\cdot 3} 5$$

Com establir la clau? (I)

- Considerem $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. Exemple: $p = 7$.
- "Treballar mòdul p" equival a l'operació `% p`.
- Existeix un generador per potències $g \in \mathbb{Z}/p\mathbb{Z}$.
- Exemple: $g = 3$.

$$3 \xrightarrow{\cdot 3} 2 \xrightarrow{\cdot 3} 6 \xrightarrow{\cdot 3} 4 \xrightarrow{\cdot 3} 5 \xrightarrow{\cdot 3} 1.$$

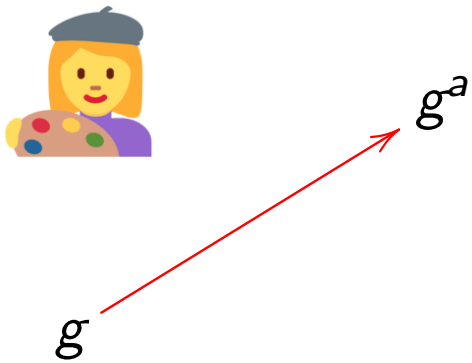
Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

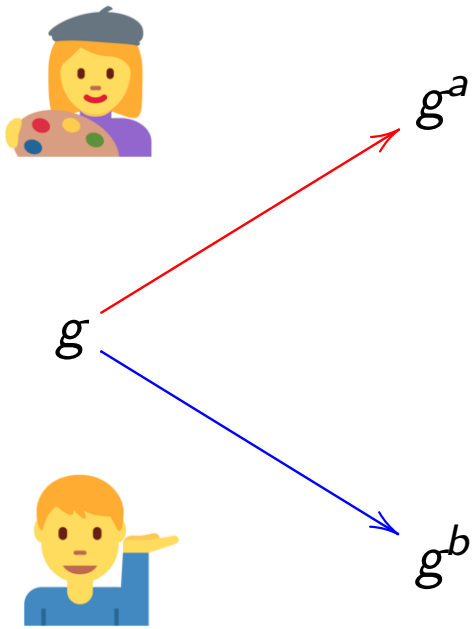
- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$.



Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

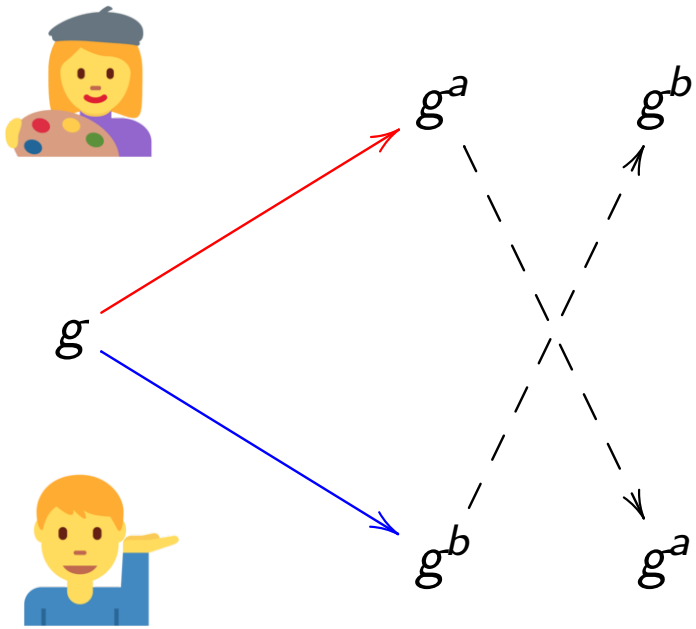
- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$.
- **Bob** tria $b \in \mathbb{Z}/p\mathbb{Z}$ i envia $B = g^b$.



Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

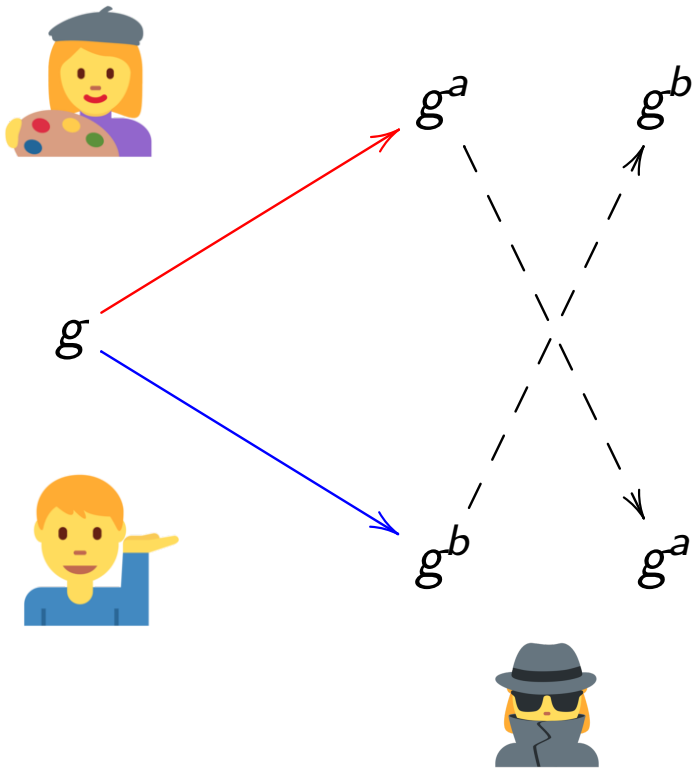
- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$.
- **Bob** tria $b \in \mathbb{Z}/p\mathbb{Z}$ i envia $B = g^b$.



Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

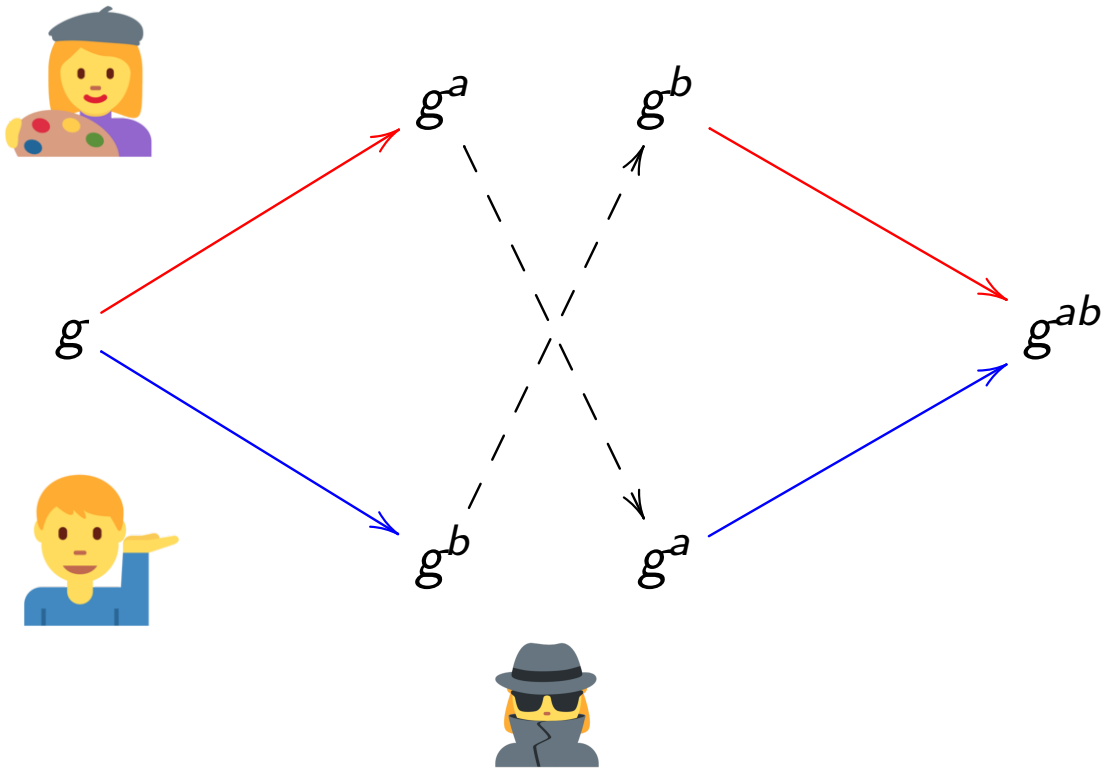
- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$.
- **Bob** tria $b \in \mathbb{Z}/p\mathbb{Z}$ i envia $B = g^b$.



Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

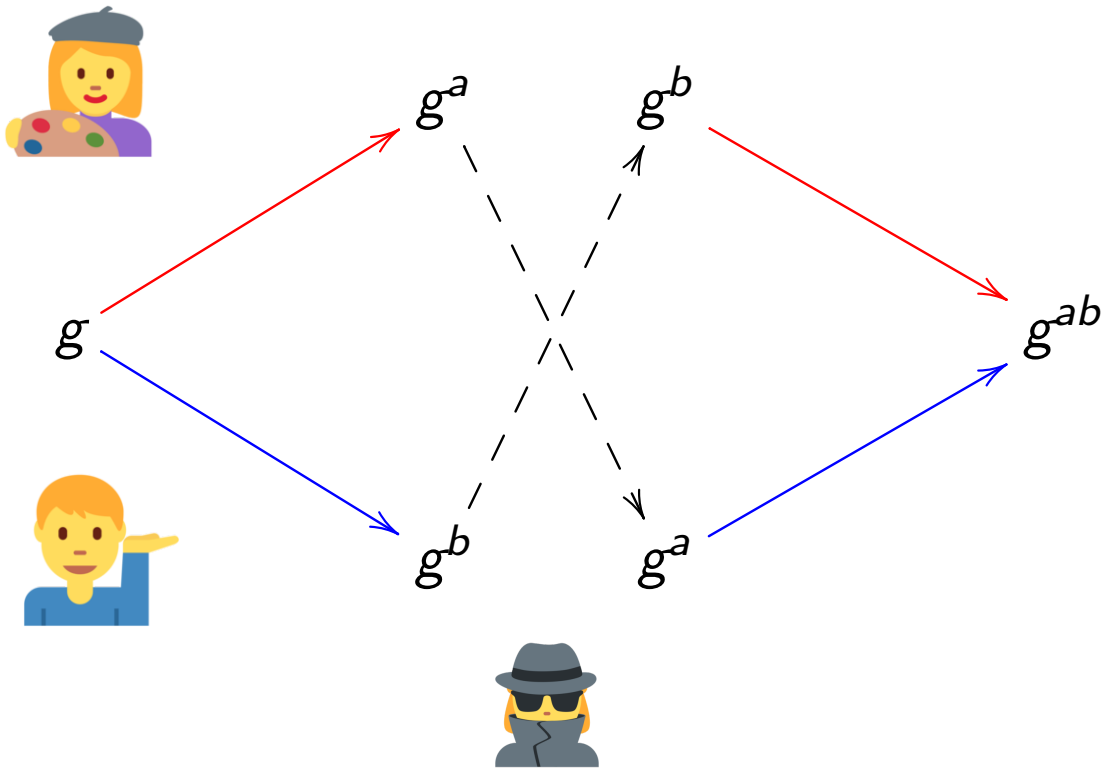
- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$.
- **Bob** tria $b \in \mathbb{Z}/p\mathbb{Z}$ i envia $B = g^b$.
- **Clau compartida**: $A^b = B^a = g^{ab}$.



Com establir la clau? (II)

Protocol Diffie-Hellman (1976):

- **Alice** tria $a \in \mathbb{Z}/p\mathbb{Z}$ i envia $A = g^a$. $a = 2,\ A = 3^2$
- **Bob** tria $b \in \mathbb{Z}/p\mathbb{Z}$ i envia $B = g^b$. $b = 5,\ A = 3^5$
- **Clau compartida**: $A^b = B^a = g^{ab}$. $(3^2)^5 = (3^5)^2 = 3^{10}$



Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

- Resoldre DLP permet trencar Diffie-Hellman.

Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

- Resoldre DLP permet trencar Diffie-Hellman.
- Millors algoritmes clàssics: subexponencials.

Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

- Resoldre DLP permet trencar Diffie-Hellman.
- Millors algoritmes clàssics: subexponencials.
- Diffie-Hellman és un **protocol segur**?

Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

- Resoldre DLP permet trencar Diffie-Hellman.
- Millors algoritmes clàssics: subexponencials.
- Diffie-Hellman és un **protocol segur**?
- Shor (1994): algoritme quàntic per resoldre DLP en temps polinòmic.

Quina seguretat té Diffie-Hellman?

Problema del logaritme discret (DLP)

Donats g i g^a, trobar l'exponent a.

- Resoldre DLP permet trencar Diffie-Hellman.
- Millors algoritmes clàssics: subexponencials.
- Diffie-Hellman és un **protocol segur**?
- Shor (1994): algoritme quàntic per resoldre DLP en temps polinòmic.
- Els **ordinadors quàntics** farien inservible la criptografia actual.

Criptografia postquàntica

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).
- NIST's Report on Post-Quantum Cryptography (2016).

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).
- NIST's Report on Post-Quantum Cryptography (2016).
- Procés d'estandardització iniciat el 2016 per l'institut NIST.

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).
- NIST's Report on Post-Quantum Cryptography (2016).
- Procés d'estandardització iniciat el 2016 per l'institut NIST.

  Criptografia basada en codis, funcions de hash, reticles, **isogènies**...

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).
- NIST's Report on Post-Quantum Cryptography (2016).
- Procés d'estandardització iniciat el 2016 per l'institut NIST.

  Criptografia basada en codis, funcions de hash, reticles, **isogènies**...
  $\sim$80 propostes inicials, 17 a la ronda 2.

Criptografia postquàntica

Requeriments de la **criptografia postquàntica**:

- Criptosistemes implementables amb el hardware actual.
- Han de ser resistents a criptoanàlisi clàssica i quàntica.

Desenvolupament:

- PQCrypto 2006: primers esforços per trobar nous algoritmes.
- PQCRYPTO EU-Project (2015 – 2018).
- NIST's Report on Post-Quantum Cryptography (2016).
- Procés d'estandardització iniciat el 2016 per l'institut NIST.

  Criptografia basada en codis, funcions de hash, reticles, **isogènies**...
  $\sim$80 propostes inicials, 17 a la ronda 2.

Entre aquestes propostes: protocol SIDH de Jao i De Feo

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.
- Presentar el protocol SIDH (Jao i De Feo, 2011).

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.
- Presentar el protocol SIDH (Jao i De Feo, 2011).
- Analitzar la seguretat del protocol SIDH, en particular:

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.
- Presentar el protocol SIDH (Jao i De Feo, 2011).
- Analitzar la seguretat del protocol SIDH, en particular:
  Atac *claw* clàssic (Adj et al., 2019)

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.
- Presentar el protocol SIDH (Jao i De Feo, 2011).
- Analitzar la seguretat del protocol SIDH, en particular:
  - Atac *claw* clàssic (Adj et al., 2019)
  - Atac actiu (Galbraith et al., 2016)

Objectius

- Desenvolupar els principis de la criptografia basada en isogènies.
- Introduir la teoria bàsica de corbes el·líptiques i isogènies.
- Presentar el protocol SIDH (Jao i De Feo, 2011).
- Analitzar la seguretat del protocol SIDH, en particular:
  - Atac *claw* clàssic (Adj et al., 2019)
  - Atac actiu (Galbraith et al., 2016)
- Implementacions en Sage de SIDH i els atacs al protocol.

Corbes el·líptiques

Definició

Una **corba el·líptica** E ve donada per una equació

$$E\colon y^2 = x^3 + Ax + B.$$

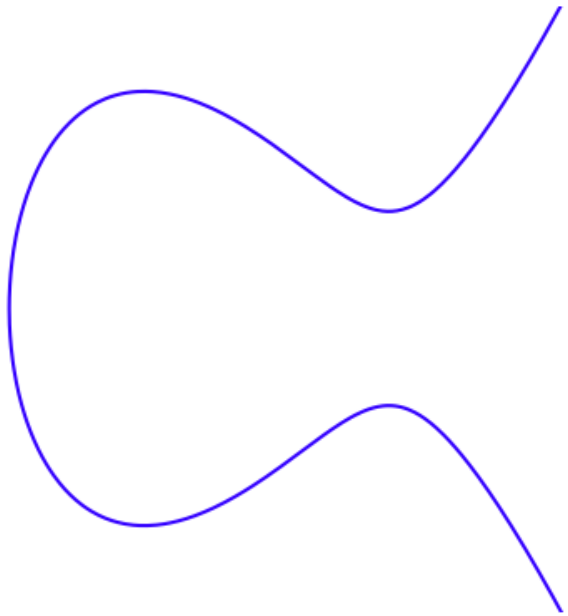
Corbes el·líptiques

Definició

Una **corba el·líptica** E ve donada per una equació

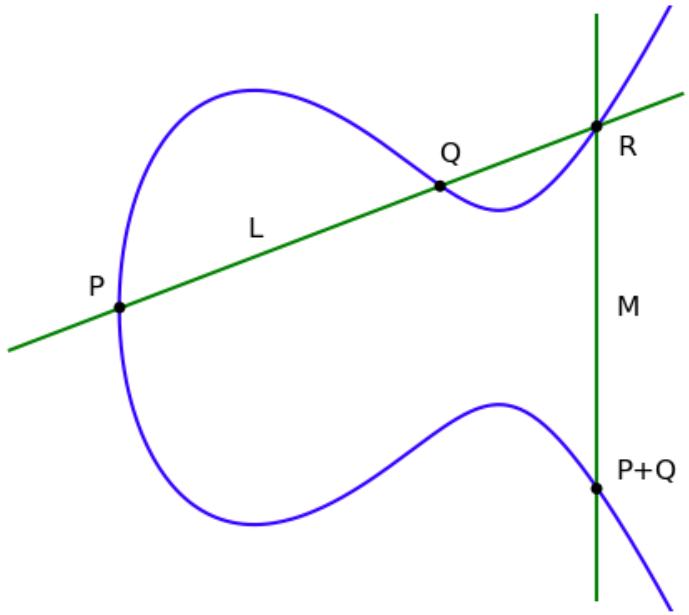
$$E\colon y^2 = x^3 + Ax + B.$$

Exemple: $y^2 = x^3 - 3x + 3$ sobre $\mathbb{R}$.



Suma de punts (I)

Donats punts P, Q de la corba, podem definir-ne la suma:



$$E\colon y^2 = x^3 - 3x + 3$$

Suma de punts (II)

Teorema

Propietats de la suma:

- Commutativa: $P + Q = Q + P$.

Suma de punts (II)

Teorema

Propietats de la suma:

- Commutativa: $P + Q = Q + P$.
- Element neutre: $P + \mathcal{O} = P$.

Suma de punts (II)

Teorema

Propietats de la suma:

- Commutativa: $P + Q = Q + P$.
- Element neutre: $P + \mathcal{O} = P$.
- Inversos: existeix $-P$, $P + (-P) = \mathcal{O}$.

Suma de punts (II)

Teorema

Propietats de la suma:

- Commutativa: $P + Q = Q + P$.
- Element neutre: $P + \mathcal{O} = P$.
- Inversos: existeix $-P$, $P + (-P) = \mathcal{O}$.
- Associativa: $(P + Q) + R = P + (Q + R)$.

Suma de punts (II)

Teorema

Propietats de la suma:

- Commutativa: $P + Q = Q + P$.
- Element neutre: $P + \mathcal{O} = P$.
- Inversos: existeix $-P$, $P + (-P) = \mathcal{O}$.
- Associativa: $(P + Q) + R = P + (Q + R)$.

L'operació $+$ dota E d'estructura de grup abelià amb neutre $\mathcal{O}$.

Invariants j: claus públiques

L'invariant j

- L'**invariant j** de E: $y^2 = x^3 + Ax + B$ es defineix com

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

L'invariant j

- L'**invariant j** de E: $y^2 = x^3 + Ax + B$ es defineix com

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

- Dues corbes són isomorfes (**equivalents**) si, i només si, tenen el mateix invariant j.

L'invariant j

- L'**invariant j** de E: $y^2 = x^3 + Ax + B$ es defineix com

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

- Dues corbes són isomorfes (**equivalents**) si, i només si, tenen el mateix invariant j.
- Per cada $j_0 \in \bar{K}$, existeix una corba E amb $j(E) = j_0$.

Isogènies: claus privades

Isogènies

Siguin E_1 i E_2 dues corbes el·líptiques.

Definició

Una **isogènia** $\phi\colon E_1 \to E_2$ és una funció de la forma

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right),$$

on $p(x), q(x), s(x), t(x)$ són polinomis,

Isogènies

Siguin E_1 i E_2 dues corbes el·líptiques.

Definició

Una **isogènia** $\phi\colon E_1 \to E_2$ és una funció de la forma

$$\phi(x,y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right),$$

on $p(x), q(x), s(x), t(x)$ són polinomis, i que compleix

$$\phi(P+Q) = \phi(P) + \phi(Q).$$

Isogènies: propietats

El **nucli** de $\phi\colon E_1 \to E_2$ és el conjunt

$$\ker \phi := \{P \in E_1 \mid \phi(P) = \mathcal{O}\}.$$

Isogènies: propietats

El **nucli** de $\phi\colon E_1 \to E_2$ és el conjunt

$$\ker \phi := \{P \in E_1 \mid \phi(P) = \mathcal{O}\}.$$

Definim el **grau** de ϕ com

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$$

$$\deg \phi := \max\{\deg p, \deg q\}.$$

Isogènies: propietats

El **nucli** de $\phi\colon E_1 \to E_2$ és el conjunt

$$\ker \phi := \{P \in E_1 \mid \phi(P) = \mathcal{O}\}.$$

Definim el **grau** de ϕ com

$$\phi(x, y) = \left(\frac{p(x)}{q(x)}, y\frac{s(x)}{t(x)}\right)$$

$$\deg \phi := \max\{\deg p, \deg q\}.$$

Teorema

$\#\ker \phi \leq \deg \phi$, més concretament:

- $\#\ker \phi = \deg \phi$ (**isogènia separable**),
- $\#\ker \phi < \deg \phi$ (**isogènia inseparable**).

Corbes quocient

Teorema

- Donat $G \subset E$ un subgrup finit, existeix una única isogènia separable

$$\phi \colon E \longrightarrow E'$$

tal que $\ker \phi = G$.

Corbes quocient

Teorema

- Donat $G \subset E$ un subgrup finit, existeix una única isogènia separable

$$\phi \colon E \longrightarrow E'$$

tal que $\ker \phi = G$.

- Càlcul amb les fórmules de Vélu en $O(\#G)$ operacions i espai $O(\#G)$.

Corbes quocient

Teorema

- Donat $G \subset E$ un subgrup finit, existeix una única isogènia separable

$$\phi \colon E \longrightarrow E'$$

tal que $\ker \phi = G$.

- Càlcul amb les fórmules de Vélu en $O(\#G)$ operacions i espai $O(\#G)$.

$$\begin{array}{c}\text{Subgrups finits}\\ \text{de } E\end{array} \quad \longleftrightarrow \quad \begin{array}{c}\text{Isogènies}\\ \text{amb domini } E\end{array}$$

Subgrups de torsió

Per cada enter $n \neq 0$, l'aplicació de multiplicació per n,

$$P \mapsto n \cdot P = P + \overset{n}{\cdots} + P$$

és una isogènia.

Subgrups de torsió

Per cada enter $n \neq 0$, l'aplicació de multiplicació per n,

$$P \mapsto n \cdot P = P + \overset{n}{\cdots} + P$$

és una isogènia.
El seu nucli és el **subgrup de n-torsió**:

$$E[n] := \ker[n] = \{P \in E \mid n \cdot P = \mathcal{O}\}.$$

Estructura de la torsió

Teorema

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Estructura de la torsió

Teorema

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Tot punt es pot expressar com $R = (a, b)$ amb $a, b \in \mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$.

Corbes el·líptiques sobre cossos finits

Si els coeficients de $y^2 = x^3 + Ax + B$ són d'un cos finit, E té un nombre finit de punts.

Corbes el·líptiques sobre cossos finits

Si els coeficients de $y^2 = x^3 + Ax + B$ són d'un cos finit, E té un nombre finit de punts.

Exemple

E: $y^2 = x^3 + x$ en $\mathbb{Z}/7\mathbb{Z}$,

$$E(\mathbb{Z}/7\mathbb{Z}) = \{(0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5), \mathcal{O}\}.$$

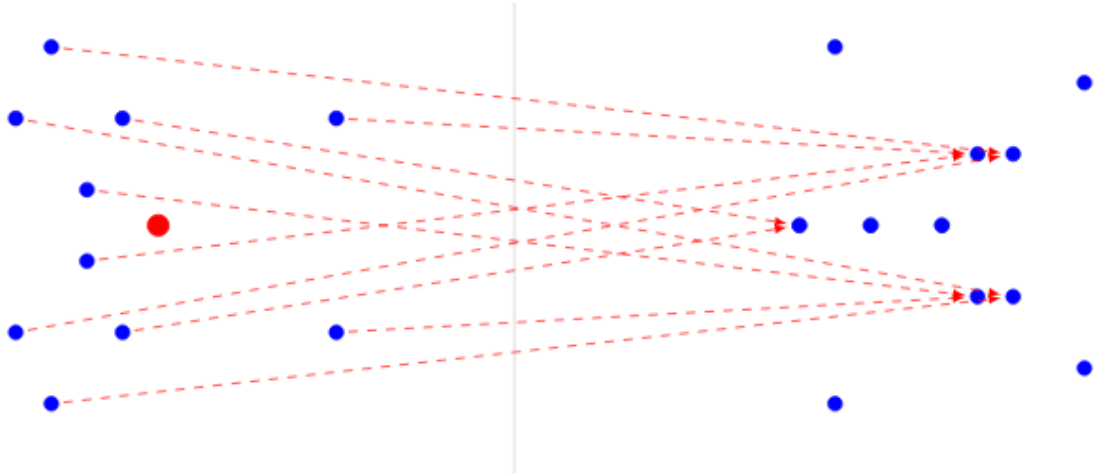
Corbes el·líptiques sobre cossos finits

Si els coeficients de $y^2 = x^3 + Ax + B$ són d'un cos finit, E té un nombre finit de punts.

Exemple

E: $y^2 = x^3 + x$ en $\mathbb{Z}/7\mathbb{Z}$,

$$E(\mathbb{Z}/7\mathbb{Z}) = \{(0,0), (1,3), (1,4), (3,3), (3,4), (5,2), (5,5), \mathcal{O}\}.$$



Corbes el·líptiques supersingulars

Definició

- E **supersingular** si:

Corbes el·líptiques supersingulars

Definició

- E **supersingular** si:
$$E[p] = \{\mathcal{O}\}.$$

Corbes el·líptiques supersingulars

Definició

- E **supersingular** si:
  $E[p] = \{\mathcal{O}\}$.
  $\#E - 1$ és divisible per p.

Corbes el·líptiques supersingulars

Definició

- E **supersingular** si:
  $E[p] = \{\mathcal{O}\}$.
  $\#E - 1$ és divisible per p.
- E **ordinària** en cas contrari.

Corbes el·líptiques supersingulars

Definició

- E **supersingular** si:
  $E[p] = \{\mathcal{O}\}$.
  $\#E - 1$ és divisible per p.
- E **ordinària** en cas contrari.

- Si E és una corba el·líptica supersingular, aleshores $j(E) \in \mathbb{F}_{p^2}$.

Corbes el·líptiques supersingulars

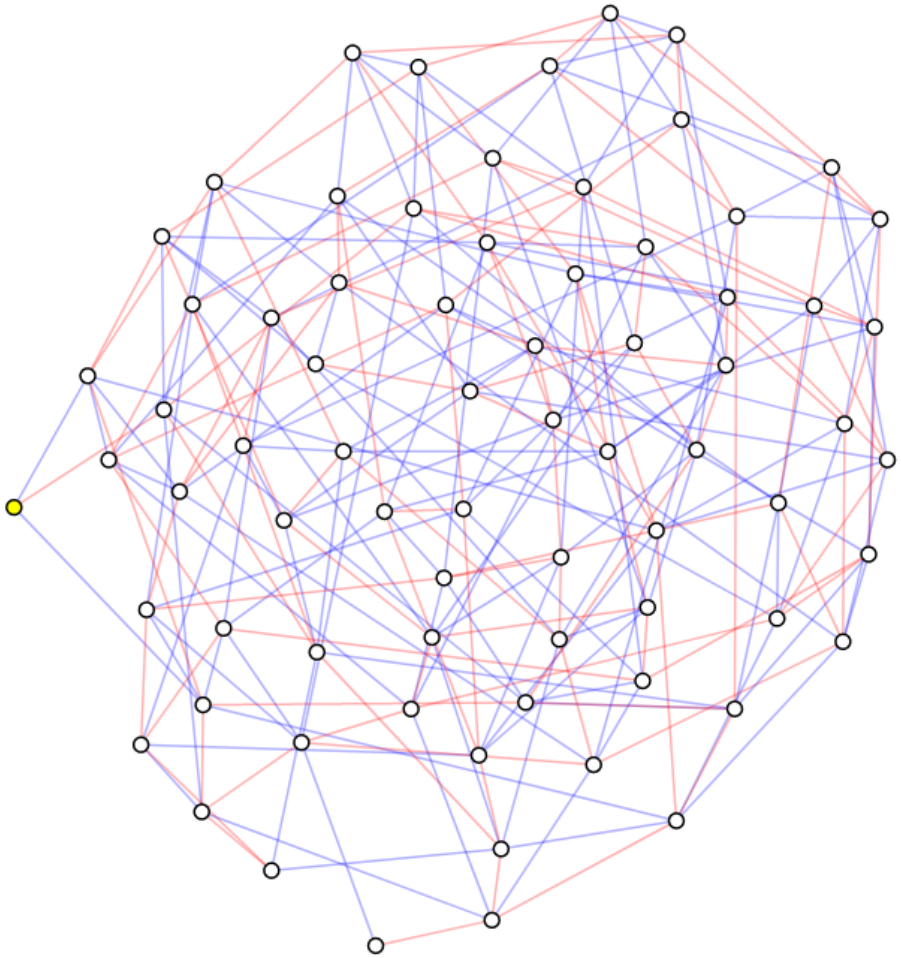
Definició

- E **supersingular** si:
  $E[p] = \{\mathcal{O}\}$.
  $\#E - 1$ és divisible per p.
- E **ordinària** en cas contrari.

- Si E és una corba el·líptica supersingular, aleshores $j(E) \in \mathbb{F}_{p^2}$.
- Donat p, existeixen $\sim p/12$ corbes el·líptiques supersingulars sobre $\mathbb{Z}/p\mathbb{Z}$.

Graf d'isogènies supersingulars

$p = 863$ (73 invariants j supersingulars)



Paràmetres del protocol

- Triem un primer $p = 2^e 3^f - 1$, $2^e \approx 3^f$.

Paràmetres del protocol

- Triem un primer $p = 2^e 3^f - 1$, $2^e \approx 3^f$.
- Corba inicial: $E_0 : y^2 = x^3 + x$, supersingular.

Paràmetres del protocol

- Triem un primer $p = 2^e 3^f - 1$, $2^e \approx 3^f$.
- Corba inicial: $E_0 : y^2 = x^3 + x$, supersingular.
- **Alice** tria un parell (m_A, n_A) mòdul 2^e.

Paràmetres del protocol

- Triem un primer $p = 2^e 3^f - 1$, $2^e \approx 3^f$.
- Corba inicial: $E_0 : y^2 = x^3 + x$, supersingular.
- **Alice** tria un parell (m_A, n_A) mòdul 2^e.
- **Bob** tria un parell (m_B, n_B) mòdul 3^f.

Intercanvi de claus SIDH

E_0

Intercanvi de claus SIDH

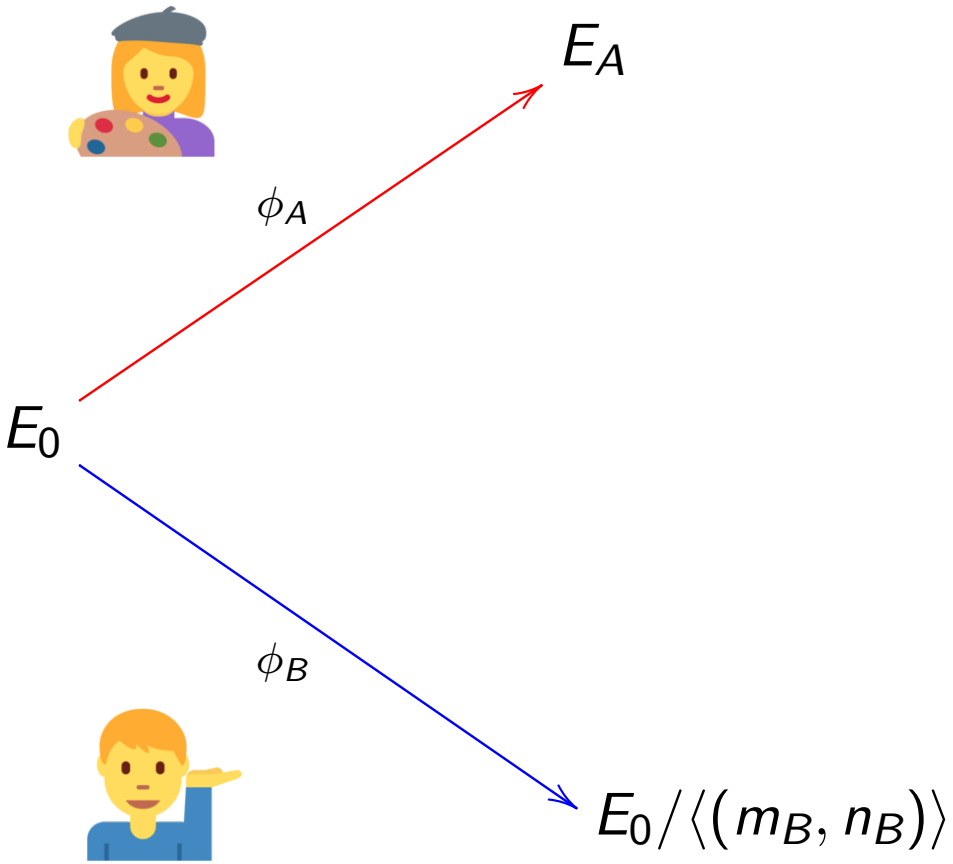
$E_0/\langle(m_A, n_A)\rangle$

ϕ_A

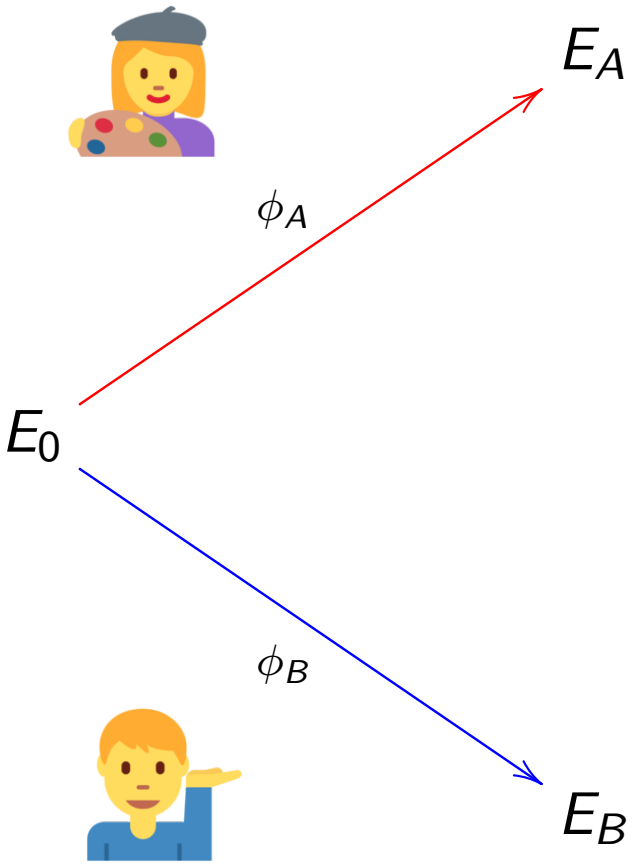
E_0

Intercanvi de claus SIDH

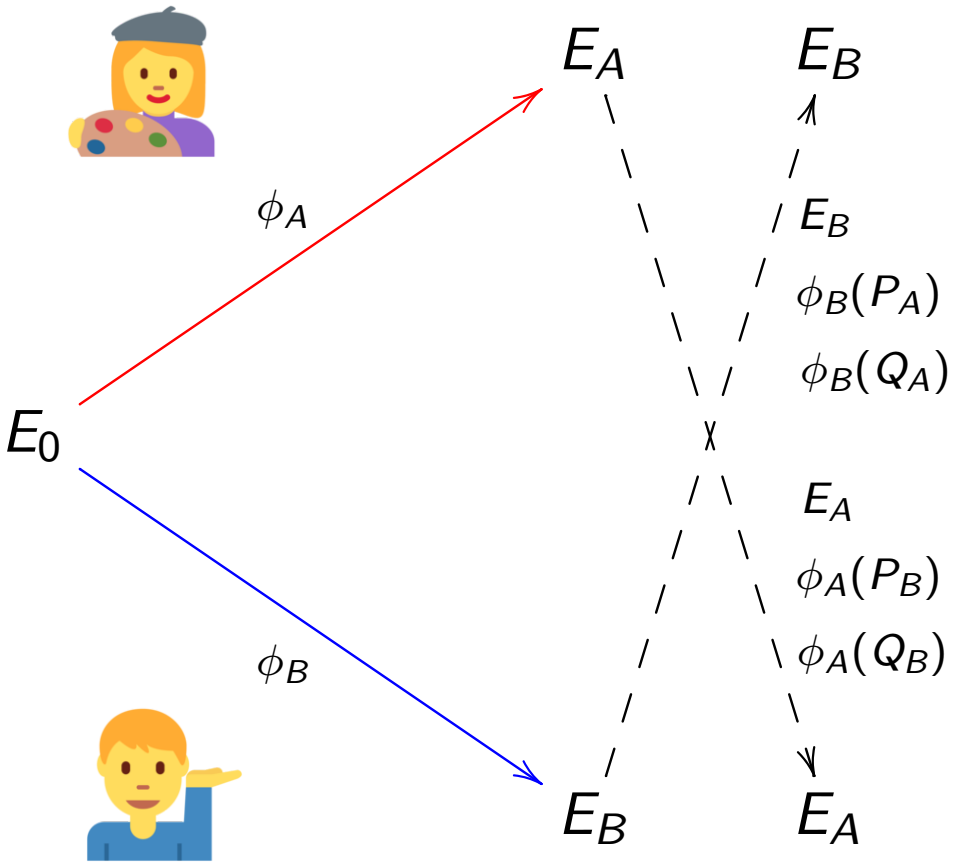
Intercanvi de claus SIDH



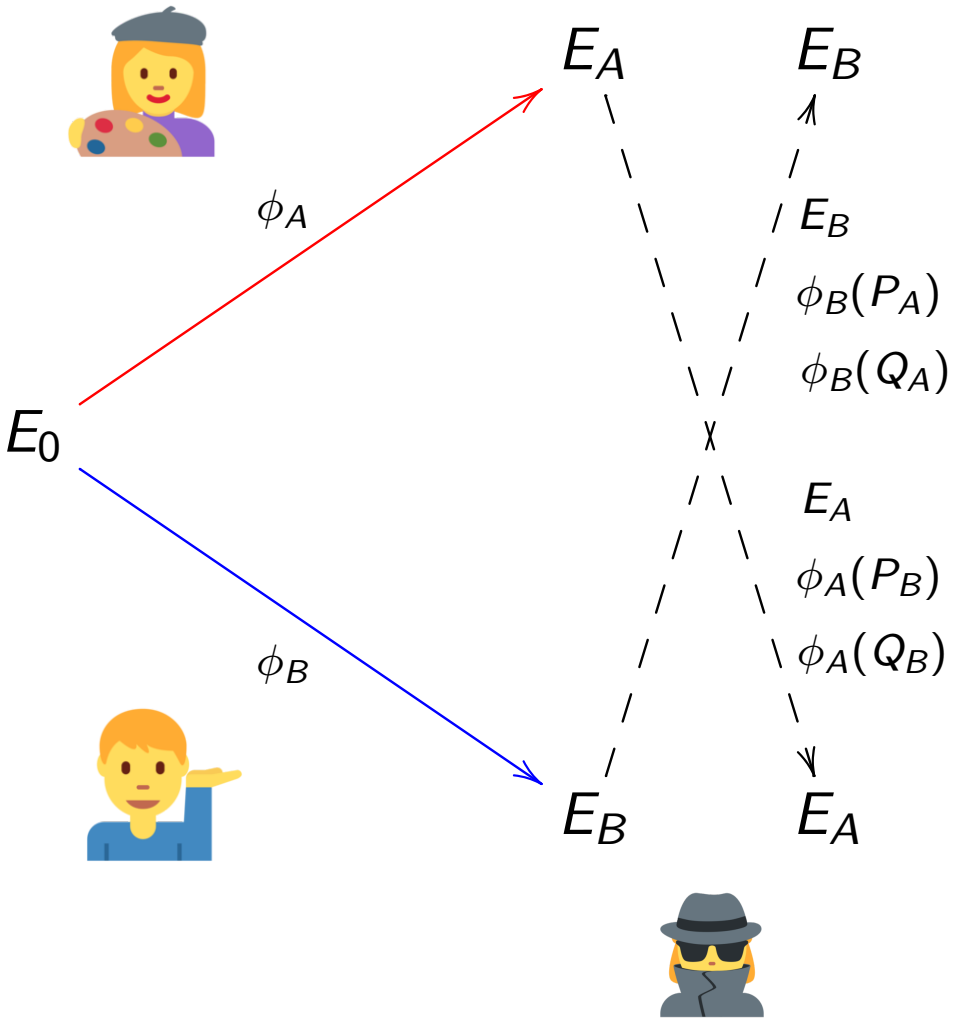
Intercanvi de claus SIDH



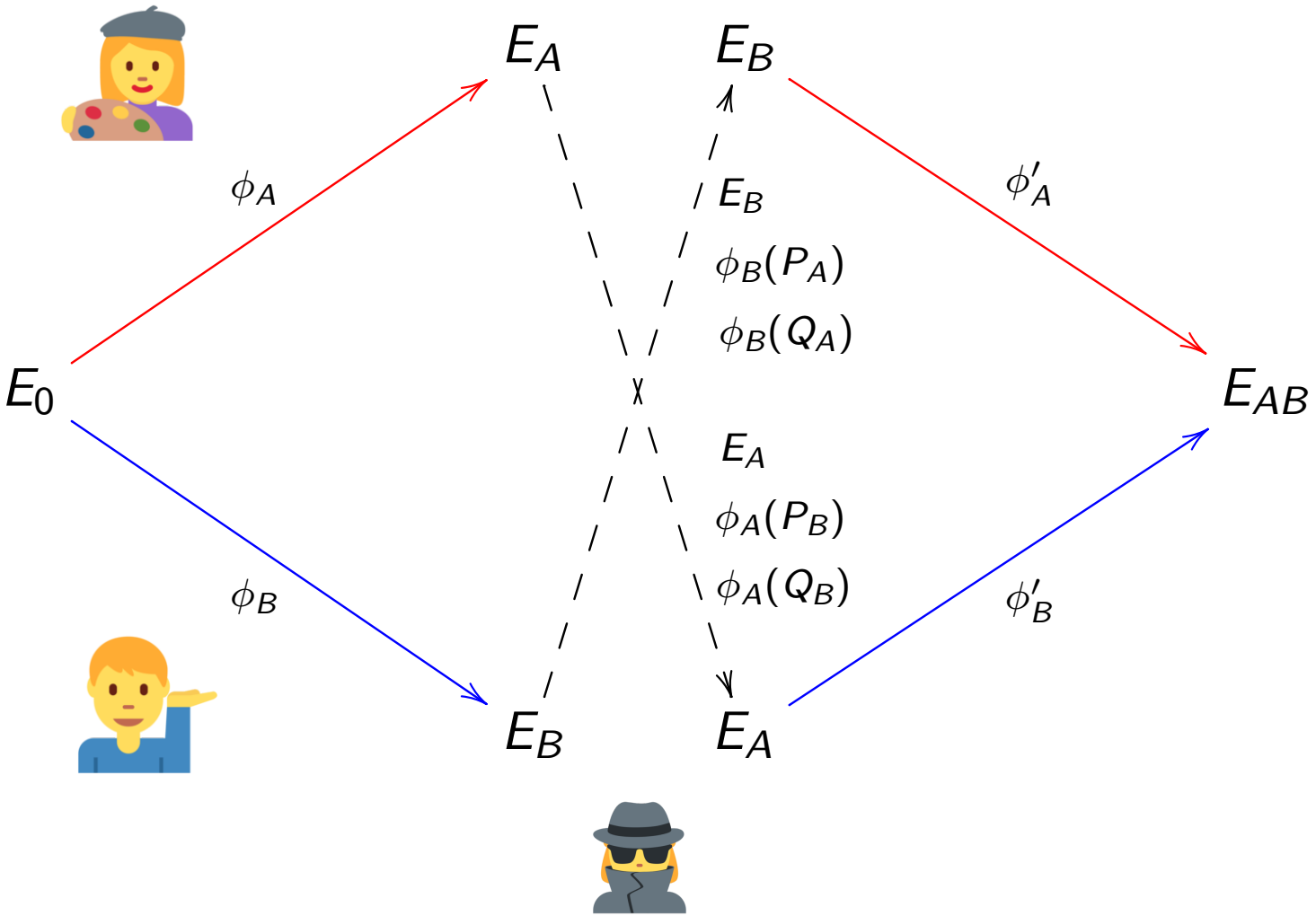
Intercanvi de claus SIDH



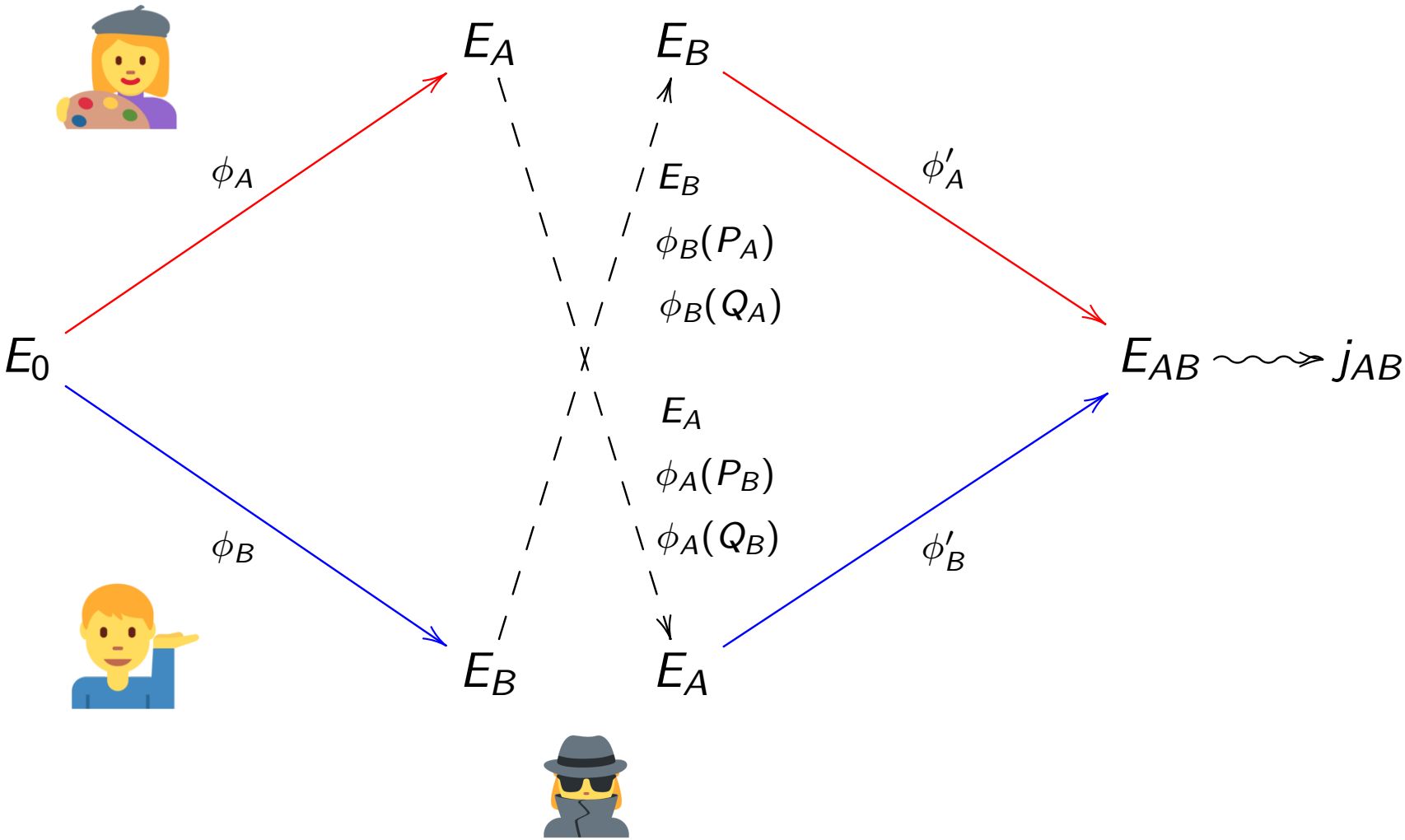
Intercanvi de claus SIDH



Intercanvi de claus SIDH

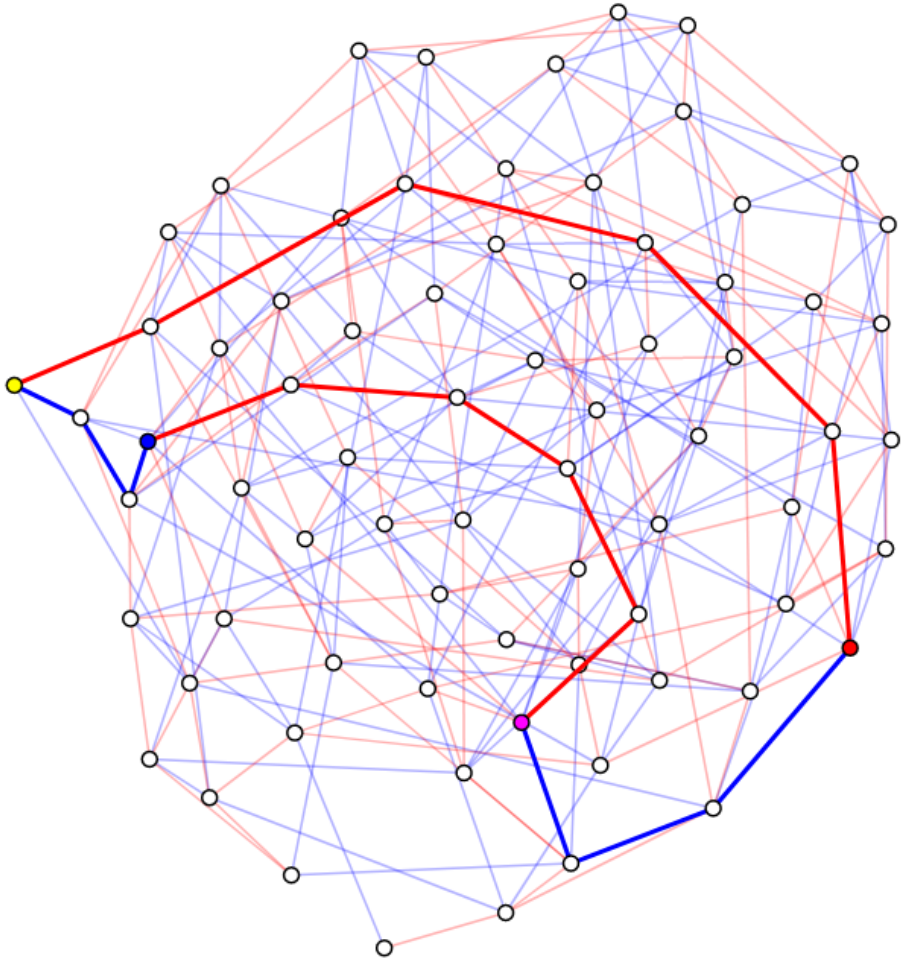


Intercanvi de claus SIDH



Visualització del SIDH

$$p = 2^5 3^3 - 1 = 863$$



Problemes computacionals

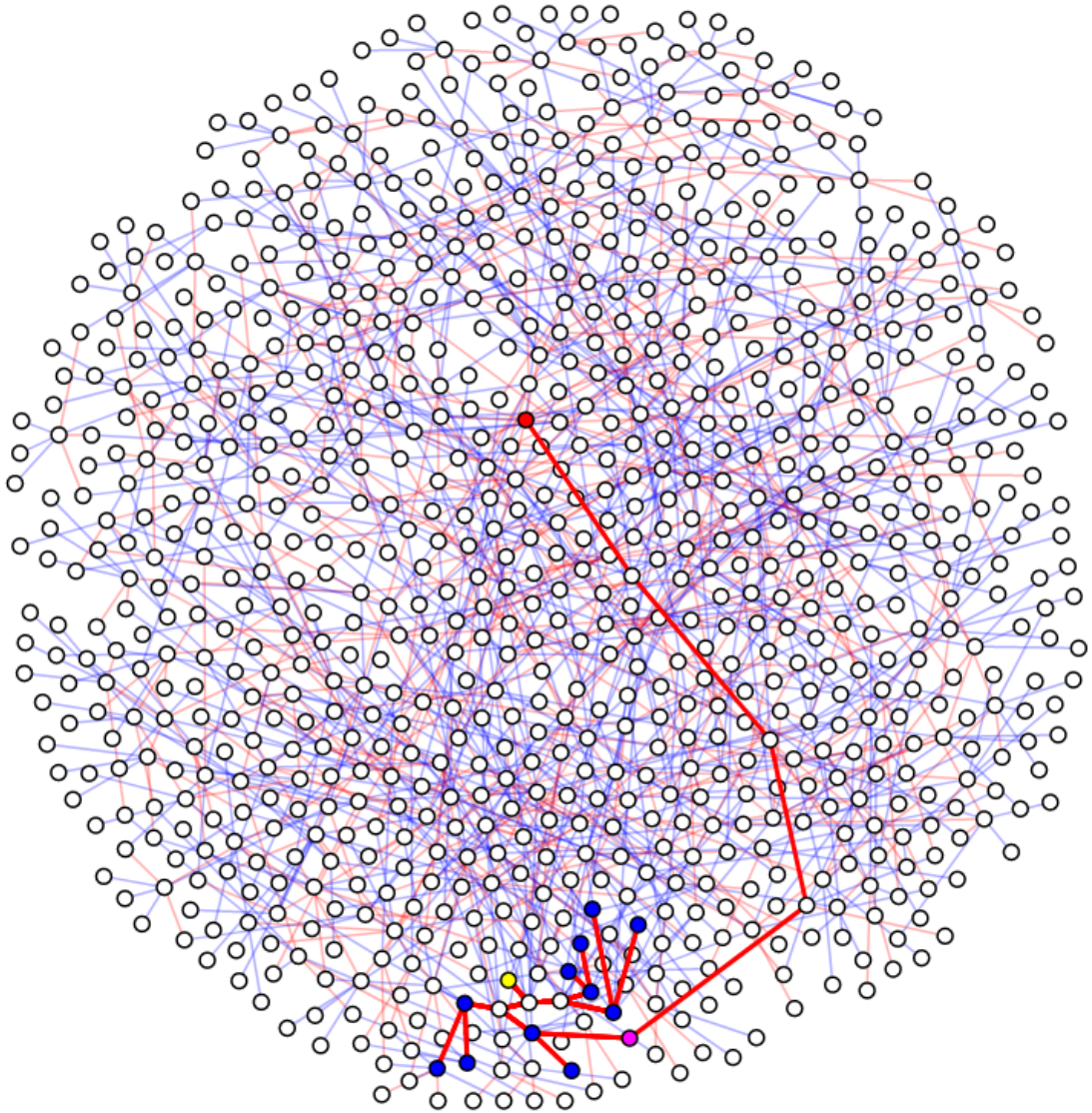
Problema de la isogènia supersingular

Donada E_0 i $(E_A, \phi_A(P_B), \phi_A(Q_B))$, trobar la isogènia secreta

$$\phi_A \colon E_0 \to E_A$$

i un generador (m, n) de $\ker \phi_A$.

Atac *claw*



Altres atacs

- Atac actiu: modificació dels punts auxiliars per obtenir informació.

Altres atacs

- Atac actiu: modificació dels punts auxiliars per obtenir informació.
- Seguretat quàntica: millor algoritme en $O(\sqrt[6]{p})$ avaluacions d'isogènies.

Implementació

- Sage: framework matemàtic sobre Python.

Implementació

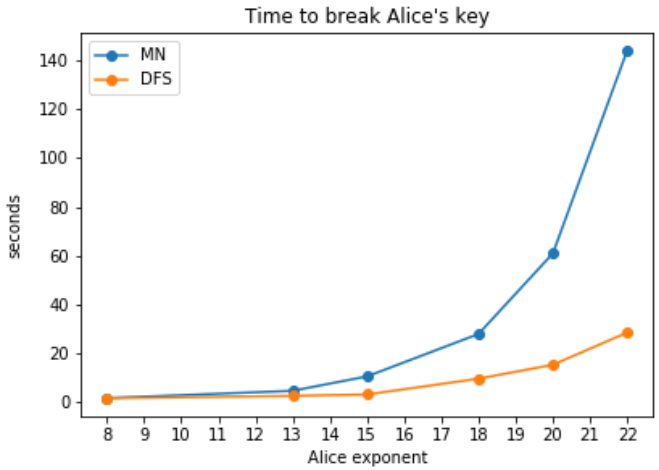
- Sage: framework matemàtic sobre Python.
- Implementació del protocol SIDH.

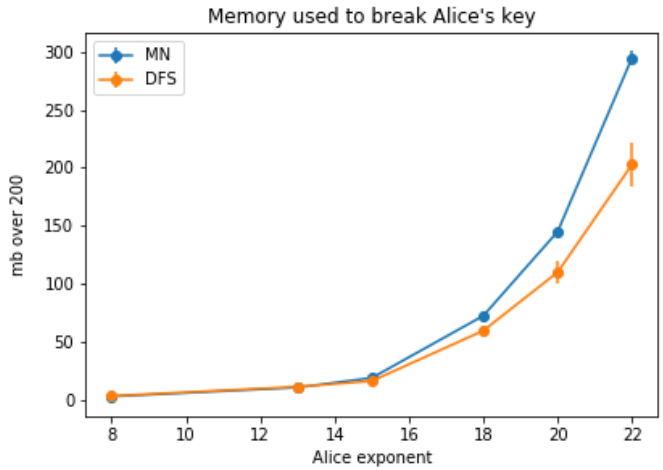
Implementació

- Sage: framework matemàtic sobre Python.
- Implementació del protocol SIDH.
- Atac *claw*: verificació del caràcter exponencial.

Implementació

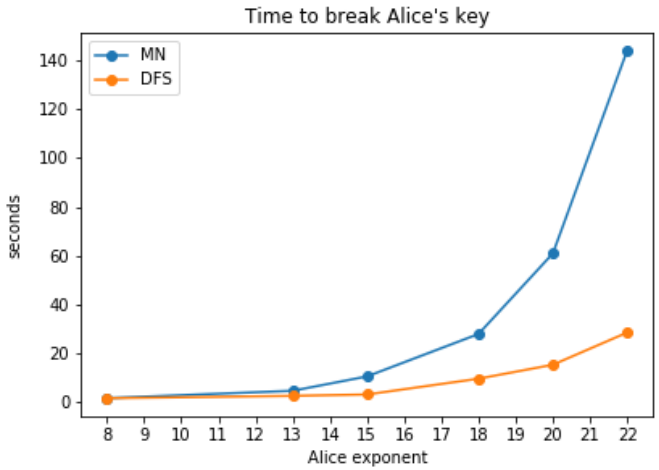
- Sage: framework matemàtic sobre Python.
- Implementació del protocol SIDH.
- Atac *claw*: verificació del caràcter exponencial.

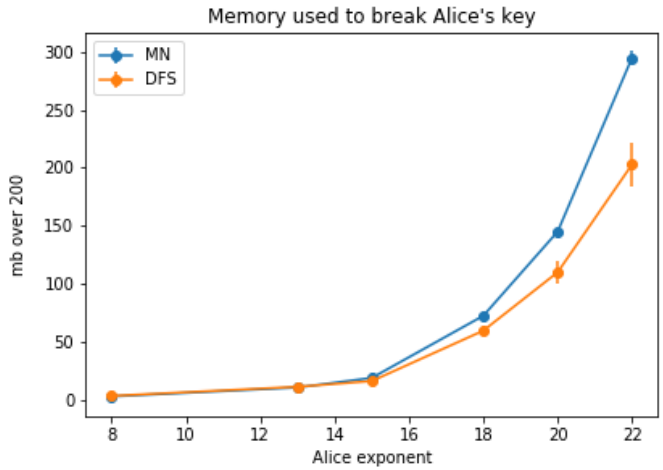




Implementació

- Sage: framework matemàtic sobre Python.
- Implementació del protocol SIDH.
- Atac *claw*: verificació del caràcter exponencial.

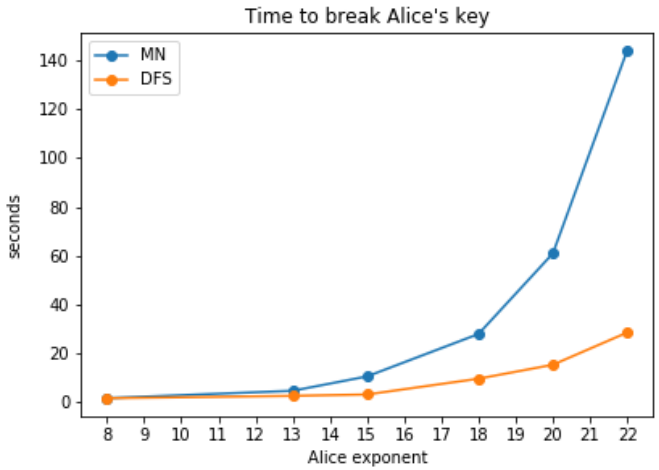


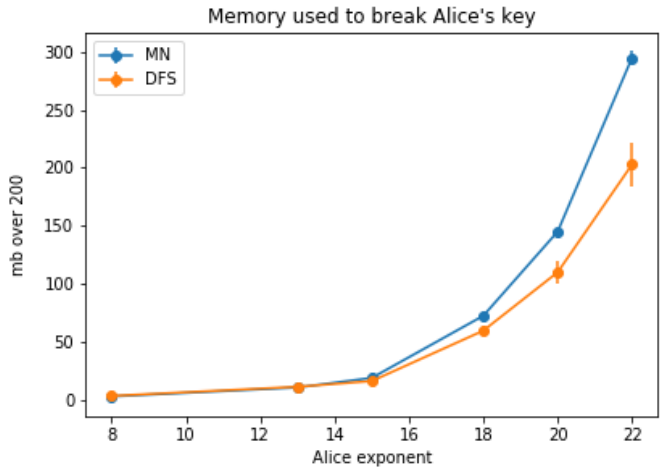


- Atac actiu (generalitzat per als casos 2^e i 3^f).

Implementació

- Sage: framework matemàtic sobre Python.
- Implementació del protocol SIDH.
- Atac *claw*: verificació del caràcter exponencial.





- Atac actiu (generalitzat per als casos 2^e i 3^f).
- Visualització dels grafs amb D3.js.

Conclusions

- Hem introduït els conceptes de la **criptografia basada en isogènies**.

Conclusions

- Hem introduït els conceptes de la **criptografia basada en isogènies**.
- SIDH és una **alternativa postquàntica eficient** als protocols Diffie-Hellman.

Conclusions

- Hem introduït els conceptes de la **criptografia basada en isogènies**.
- SIDH és una **alternativa postquàntica eficient** als protocols Diffie-Hellman.
- Atac *claw* clàssic en $O(\sqrt[4]{p})$ i millor atac quàntic en $O(\sqrt[6]{p})$ avaluacions d'isogènies.

Extensions del treball

- Generalització de l'atac *claw* a isogènies de grau arbitrari compost N (en progrés).

Extensions del treball

- Generalització de l'atac *claw* a isogènies de grau arbitrari compost N (en progrés).
- CSIDH: protocol basat en multiplicació complexa.

Extensions del treball

- Generalització de l'atac *claw* a isogènies de grau arbitrari compost N (en progrés).
- CSIDH: protocol basat en multiplicació complexa.
- Altres esquemes criptogràfics: funcions de hash, signatures digitals...

Extensions del treball

- Generalització de l'atac *claw* a isogènies de grau arbitrari compost N (en progrés).
- CSIDH: protocol basat en multiplicació complexa.
- Altres esquemes criptogràfics: funcions de hash, signatures digitals...
- Canviar les corbes el·líptiques per varietats jacobianes de corbes hiperel·líptiques (Institut Inria a París, març - juny 2020).

Referències

[Sut] Andrew Sutherland. *18.783 Elliptic Curves, 2017*. MIT OpenCourseWare.

[FJP11] Luca De Feo, David Jao i Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. 2011.

[Gal+16] Steven D. Galbraith et al. *On the Security of Supersingular Isogeny Cryptosystems*. 2016.

[Adj+19] Gora Adj et al. *On the Cost of Computing Isogenies Between Supersingular Elliptic Curves*. 2019.

[Sag19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. `https://www.sagemath.org`. 2019.

Criptografia basada en isogènies

Enric Florit Zacarías

Directors: Xavier Guitart, Santiago Seguí i Ramsès Fernàndez

Departament de Matemàtiques i Informàtica – Universitat de Barcelona
Departament d'ITSecurity – Fundació Eurecat

7 de febrer de 2020