Criptografía basada en isogenias

Amalia Pizarro Madariaga

Instituto de Matemáticas
Universidad de Valparaíso

Seminario Latinoamericano de Teoría de Números

Secretos Compartidos: Protocolo de Diffie-Hellman ’76 [8]

- $(G, \cdot)$ grupo abeliano finito actuando sobre un conjunto S via $*$ y $s_0 \in S$ elemento fijo.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

- $(G, \cdot)$ grupo abeliano finito actuando sobre un conjunto S via $*$ y $s_0 \in S$ elemento fijo.
- Alice y Bob escogen a y b en G aleatorios.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

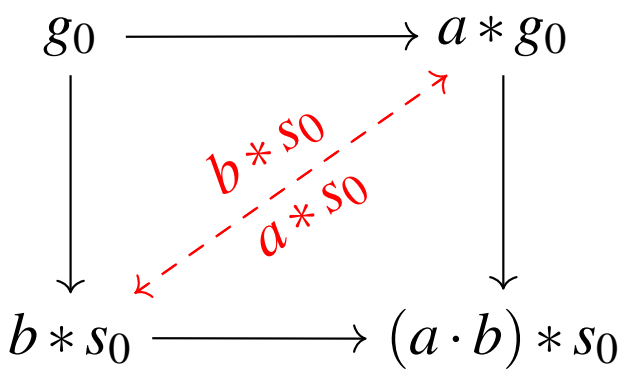
- $(G, \cdot)$ grupo abeliano finito actuando sobre un conjunto S via $*$ y $s_0 \in S$ elemento fijo.
- Alice y Bob escogen a y b en G aleatorios.
- Calculan $a * g_0$ y $b * g_0$ y los hacen públicos.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

- $(G, \cdot)$ grupo abeliano finito actuando sobre un conjunto S via $*$ y $s_0 \in S$ elemento fijo.
- Alice y Bob escogen a y b en G aleatorios.
- Calculan $a * g_0$ y $b * g_0$ y los hacen públicos.
- Secreto compartido: $(a \cdot b) * s_0$.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

- $(G, \cdot)$ grupo abeliano finito actuando sobre un conjunto S via $*$ y $s_0 \in S$ elemento fijo.
- Alice y Bob escogen a y b en G aleatorios.
- Calculan $a * g_0$ y $b * g_0$ y los hacen públicos.
- Secreto compartido: $(a \cdot b) * s_0$.



Secretos Compartidos: Protocolo de Diffie-Hellman ’76 [8]

- Sea G es un grupo abeliano finito (por ejemplo $\mathbb{F}_p^*$ o $E(\mathbb{F}_p)$) con generador g_0

Secretos Compartidos: Protocolo de Diffie-Hellman ’76 [8]

- Sea G es un grupo abeliano finito (por ejemplo $\mathbb{F}_p^*$ o $E(\mathbb{F}_p)$) con generador g_0
- Alice y Bob escogen a y b en enteros aleatorios.

Secretos Compartidos: Protocolo de Diffie-Hellman ’76 [8]

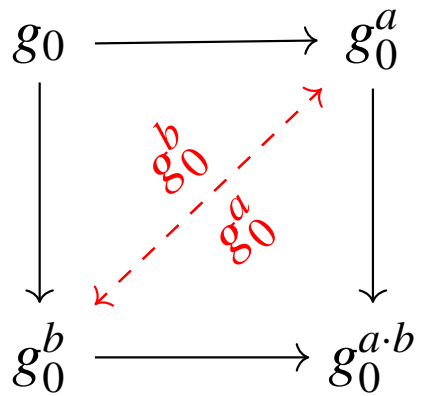
- Sea G es un grupo abeliano finito (por ejemplo $\mathbb{F}_p^*$ o $E(\mathbb{F}_p)$) con generador g_0
- Alice y Bob escogen a y b en enteros aleatorios.
- Calculan g_0^a y g_0^b y los hacen públicos.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

- Sea G es un grupo abeliano finito (por ejemplo $\mathbb{F}_p^*$ o $E(\mathbb{F}_p)$) con generador g_0
- Alice y Bob escogen a y b en enteros aleatorios.
- Calculan g_0^a y g_0^b y los hacen públicos.
- Secreto compartido: $g^{a \cdot b}$.

Secretos Compartidos: Protocolo de Diffie-Hellman '76 [8]

- Sea G es un grupo abeliano finito (por ejemplo $\mathbb{F}_p^*$ o $E(\mathbb{F}_p)$) con generador g_0
- Alice y Bob escogen a y b en enteros aleatorios.
- Calculan g_0^a y g_0^b y los hacen públicos.
- Secreto compartido: $g^{a\cdot b}$.



Curvas Elípticas sobre cuerpos finitos

- La ecuación (corta) de Weierstrass de una curva elíptica está dada por,

$$E : y^2 = x^3 + ax + b,$$

con $a, b \in \mathbb{F}_q$, $q = p^\ell$, con p primo $p \neq 2, 3$ y $4a^3 + 27b^2 \neq 0$.

Curvas Elípticas sobre cuerpos finitos

- La ecuación (corta) de Weierstrass de una curva elíptica está dada por,

$$E : y^2 = x^3 + ax + b,$$

con $a, b \in \mathbb{F}_q$, $q = p^\ell$, con p primo $p \neq 2, 3$ y $4a^3 + 27b^2 \neq 0$.

- Dados P y Q dos puntos en la curva, existe una construcción geométrica para la adición $P + Q$.

Curvas Elípticas sobre cuerpos finitos

- La ecuación (corta) de Weierstrass de una curva elíptica está dada por,

$$E : y^2 = x^3 + ax + b,$$

con $a, b \in \mathbb{F}_q$, $q = p^\ell$, con p primo $p \neq 2, 3$ y $4a^3 + 27b^2 \neq 0$.

- Dados P y Q dos puntos en la curva, existe una construcción geométrica para la adición $P + Q$.
- Denotamos por $E(\mathbb{F}_q)$ al conjunto de puntos (x, y) de la curva con coordenadas en $\mathbb{F}_q$,junto con un "punto en el infinito" O. Forman un grupo abeliano con la adición.

Curvas Elípticas sobre cuerpos finitos

- La ecuación (corta) de Weierstrass de una curva elíptica está dada por,

$$E : y^2 = x^3 + ax + b,$$

con $a, b \in \mathbb{F}_q$, $q = p^\ell$, con p primo $p \neq 2, 3$ y $4a^3 + 27b^2 \neq 0$.

- Dados P y Q dos puntos en la curva, existe una construcción geométrica para la adición $P + Q$.
- Denotamos por $E(\mathbb{F}_q)$ al conjunto de puntos (x, y) de la curva con coordenadas en $\mathbb{F}_q$,junto con un "punto en el infinito" O. Forman un grupo abeliano con la adición.
- Teorema de Hasse: $\#E(\mathbb{F}_q) = q + 1 - t_q$, con $|t_q| \leq 2\sqrt{q}$.

Criptografía con Curvas Elípticas

- Problema del logaritmo discreto: Dado $g \in G$, calcular x tal que $g_0^x = g$.

Criptografía con Curvas Elípticas

- Problema del logaritmo discreto: Dado $g \in G$, calcular x tal que $g_0^x = g$.
- Desde 1985, se han desarrollado diversos protocolos criptográficos basados en el protocolo de intercambio de claves de Diffie-Hellman con curvas elípticas.

Criptografía con Curvas Elípticas

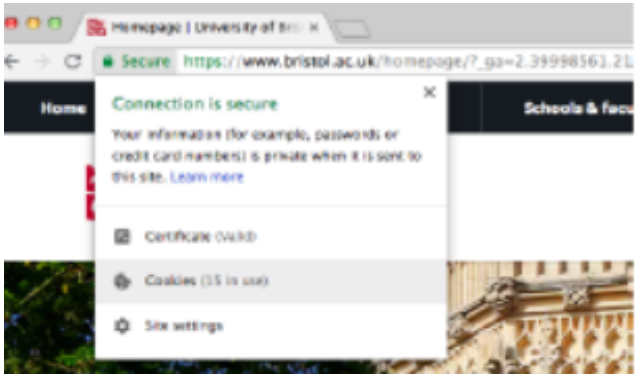
- Problema del logaritmo discreto: Dado $g \in G$, calcular x tal que $g_0^x = g$.
- Desde 1985, se han desarrollado diversos protocolos criptográficos basados en el protocolo de intercambio de claves de Diffie-Hellman con curvas elípticas.
- Esquemas de firmas digitales (app bancarias, sitios web seguros)

Criptografía con Curvas Elípticas

- Problema del logaritmo discreto: Dado $g \in G$, calcular x tal que $g_0^x = g$.
- Desde 1985, se han desarrollado diversos protocolos criptográficos basados en el protocolo de intercambio de claves de Diffie-Hellman con curvas elípticas.
- Esquemas de firmas digitales (app bancarias, sitios web seguros)
- Servicios de mensajería encriptados (eg. WhatsApp; Signal; WireGuard).

Criptografía con Curvas Elípticas

- Problema del logaritmo discreto: Dado $g \in G$, calcular x tal que $g_0^x = g$.
- Desde 1985, se han desarrollado diversos protocolos criptográficos basados en el protocolo de intercambio de claves de Diffie-Hellman con curvas elípticas.
- Esquemas de firmas digitales (app bancarias, sitios web seguros)
- Servicios de mensajería encriptados (eg. WhatsApp; Signal; WireGuard).



Niveles de seguridad

- El mejor algoritmo conocido para resolver ECDLP es de Pollard, que lo resuelve en $O(\sqrt{\#E(\mathbb{F}_p)})$ pasos.

Niveles de seguridad

- El mejor algoritmo conocido para resolver ECDLP es de Pollard, que lo resuelve en $O(\sqrt{\#E(\mathbb{F}_p)})$ pasos.
- Se asume que sobre 2^{80} operaciones elementales, es una cantidad inviable de cómputos.

Niveles de seguridad

- El mejor algoritmo conocido para resolver ECDLP es de Pollard, que lo resuelve en $O(\sqrt{\#E(\mathbb{F}_p)})$ pasos.
- Se asume que sobre 2^{80} operaciones elementales, es una cantidad inviable de cómputos.
- Se dice que un criptosistema tiene nivel de seguridad q, si el mejor ataque conocido toma $O(2^q)$ operaciones elementales.

Niveles de seguridad

- El mejor algoritmo conocido para resolver ECDLP es de Pollard, que lo resuelve en $O(\sqrt{\#E(\mathbb{F}_p)})$ pasos.
- Se asume que sobre 2^{80} operaciones elementales, es una cantidad inviable de cómputos.
- Se dice que un criptosistema tiene nivel de seguridad q, si el mejor ataque conocido toma $O(2^q)$ operaciones elementales.
- En 1999, NIST recomendó 5 cuerpos finitos $\mathbb{F}_p$ para ciertos primos p de tamaño 192, 224, 256, 384, y 521 bits, con curvas específicas recomendadas.

Niveles de seguridad

- El mejor algoritmo conocido para resolver ECDLP es de Pollard, que lo resuelve en $O(\sqrt{\#E(\mathbb{F}_p)})$ pasos.
- Se asume que sobre 2^{80} operaciones elementales, es una cantidad inviable de cómputos.
- Se dice que un criptosistema tiene nivel de seguridad q, si el mejor ataque conocido toma $O(2^q)$ operaciones elementales.
- En 1999, NIST recomendó 5 cuerpos finitos $\mathbb{F}_p$ para ciertos primos p de tamaño 192, 224, 256, 384, y 521 bits, con curvas específicas recomendadas.
- En la actualidad, las claves utilizadas para RSA son de tamaño 1024 bits a 2048, mientras que para ECC son de 256 bits.

Criptografía Postcuántica

En 1997: El Algoritmo de Shor [19] (cuántico) resuelve el problema del logaritmo discreto y de factorización de enteros en tiempo polinomial.

En Agosto de 2015 NSA anuncia un plan de transición hacia algoritmo resistentes a la computación cuántica.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

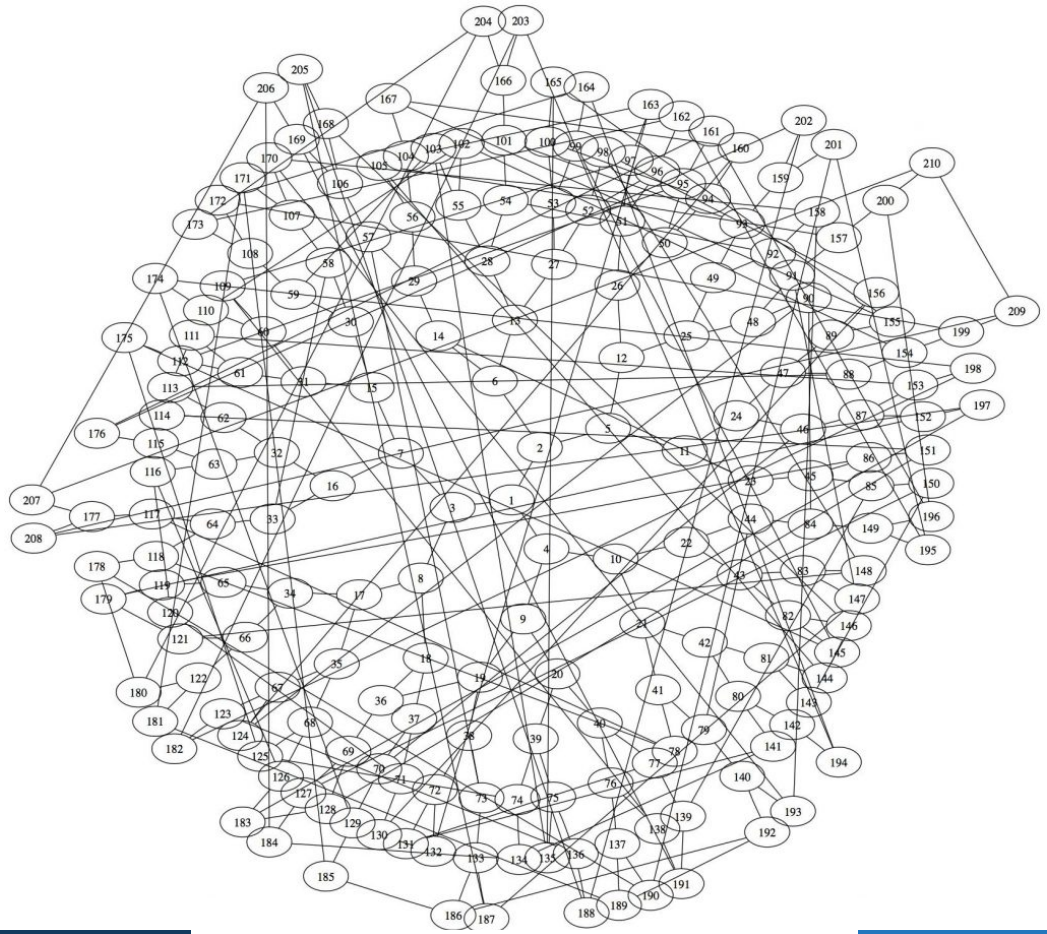
En 2016 NIST [15] convoca un concurso con límite Nov 2017 para someter algoritmos criptográficos post-cuánticos.

Criptografía Basada en Isogenias

Grafo de isogenias:

Vértices: j-invariantes de curvas isogenas

Aristas: isogenias entre curvas elípticas



Criptografía Basada en Isogenias

- 1996 Couveignes [7]: Primer esquema basado en isogenias.

Criptografía Basada en Isogenias

- 1996 Couveignes [7]: Primer esquema basado en isogenias.
- 2006 Rostovtsev y Stolbunov [18], (2010) Stolbunov: protocolo de intercambio de claves utilizando isogenias *ordinarias*.

Criptografía Basada en Isogenias

- 1996 Couveignes [7]: Primer esquema basado en isogenias.
- 2006 Rostovtsev y Stolbunov [18], (2010) Stolbunov: protocolo de intercambio de claves utilizando isogenias *ordinarias*.
- 2006 Funciones hash en grafos supersingulares: Charles, Goren y Lauter [3].

Criptografía Basada en Isogenias

- 1996 Couveignes [7]: Primer esquema basado en isogenias.
- 2006 Rostovtsev y Stolbunov [18], (2010) Stolbunov: protocolo de intercambio de claves utilizando isogenias *ordinarias*.
- 2006 Funciones hash en grafos supersingulares: Charles, Goren y Lauter [3].
- 2010 Childs, Jao and Soukharev: ataque (cuántico) en tiempo subexponential.

Criptografía Basada en Isogenias

- 1996 Couveignes [7]: Primer esquema basado en isogenias.
- 2006 Rostovtsev y Stolbunov [18], (2010) Stolbunov: protocolo de intercambio de claves utilizando isogenias *ordinarias*.
- 2006 Funciones hash en grafos supersingulares: Charles, Goren y Lauter [3].
- 2010 Childs, Jao and Soukharev: ataque (cuántico) en tiempo subexponential.
- 2011 Jao y De Feo [13]: intercambio de claves utilizando isogenias *supersingulares* (SIDH).

Curvas Elípticas sobre cuerpos finitos II

- Una isogenia ϕ entre dos curvas elípticas E_1 y E_2 preserva la ley de grupo, es una función racional y $\phi(O_1) = O_2$. Una isogenia es siempre sobreyectiva.

Curvas Elípticas sobre cuerpos finitos II

- Una isogenia ϕ entre dos curvas elípticas E_1 y E_2 preserva la ley de grupo, es una función racional y $\phi(O_1) = O_2$. Una isogenia es siempre sobreyectiva.
- Grado de una isogenia corresponde al grado de una de las funciones racionales involucradas.

Curvas Elípticas sobre cuerpos finitos II

- Una isogenia ϕ entre dos curvas elípticas E_1 y E_2 preserva la ley de grupo, es una función racional y $\phi(O_1) = O_2$. Una isogenia es siempre sobreyectiva.
- Grado de una isogenia corresponde al grado de una de las funciones racionales involucradas.
- Isomorfismo de curvas elípticas: Isogenias inyectivas, i.e. con kernel trivial.

Curvas Elípticas sobre cuerpos finitos II

- Una isogenia ϕ entre dos curvas elípticas E_1 y E_2 preserva la ley de grupo, es una función racional y $\phi(O_1) = O_2$. Una isogenia es siempre sobreyectiva.
- Grado de una isogenia corresponde al grado de una de las funciones racionales involucradas.
- Isomorfismo de curvas elípticas: Isogenias inyectivas, i.e. con kernel trivial.
- j-invariante de E: $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$.

Curvas Elípticas sobre cuerpos finitos II

- Una isogenia ϕ entre dos curvas elípticas E_1 y E_2 preserva la ley de grupo, es una función racional y $\phi(O_1) = O_2$. Una isogenia es siempre sobreyectiva.
- Grado de una isogenia corresponde al grado de una de las funciones racionales involucradas.
- Isomorfismo de curvas elípticas: Isogenias inyectivas, i.e. con kernel trivial.
- j-invariante de E: $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$.
- Dos curvas son isomorfas en $\overline{\mathbb{F}}_q$ si y solo si sus j-invariantes son iguales.

Isogenias

- Consideraremos isogenias separables :$|ker\phi|$=deg ϕ.

Isogenias

- Consideraremos isogenias separables :$|ker\phi|$=deg ϕ.
- Una isogenia $\phi : E \to E$ es llamada un endomorfismo.

Isogenias

- Consideraremos isogenias separables :$|ker\phi|$=deg ϕ.
- Una isogenia $\phi : E \to E$ es llamada un endomorfismo.
- Multiplicación por ℓ: $[\ell] : E \to E$, $P \mapsto \ell P$.

Isogenias

- Consideraremos isogenias separables :$|ker\phi|$=deg ϕ.
- Una isogenia $\phi : E \to E$ es llamada un endomorfismo.
- Multiplicación por ℓ: $[\ell] : E \to E$, $P \mapsto \ell P$.
- Isogenias separables están completamente determinadas por su kernel: dado un subgrupo finito G de $E_1(\mathbb{F}_q)$, existen única (salvo isomorfismo) curva elíptica E_2 e isogenia $\phi : E_1 \to E_2$ con $ker\phi = G$. Escribimos $E_2 = \phi(E_1) = E_1/\langle G \rangle$.

Isogenias

- Consideraremos isogenias separables :$|ker\phi|$=deg ϕ.
- Una isogenia $\phi : E \to E$ es llamada un endomorfismo.
- Multiplicación por ℓ: $[\ell] : E \to E$, $P \mapsto \ell P$.
- Isogenias separables están completamente determinadas por su kernel: dado un subgrupo finito G de $E_1(\mathbb{F}_q)$, existen única (salvo isomorfismo) curva elíptica E_2 e isogenia $\phi : E_1 \to E_2$ con $ker\phi = G$. Escribimos $E_2 = \phi(E_1) = E_1/\langle G \rangle$.
- Teorema de Tate: Dos curvas elípticas E_1 y E_2 son isogenas sobre $\mathbb{F}_q$ si y solo si $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Subgrupos de Torsión

- Subgrupo de n-torsión

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) : [n]P = O\} = ker[n].$$

Subgrupos de Torsión

- Subgrupo de n-torsión

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) : [n]P = O\} = ker[n].$$

- Si ϕ es una isogenia, entonces

$$ker\phi \subseteq ker[n] = E[n].$$

Subgrupos de Torsión

- Subgrupo de n-torsión

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) : [n]P = O\} = ker[n].$$

- Si ϕ es una isogenia, entonces

$$ker\phi \subseteq ker[n] = E[n].$$

- **Estructura del subgrupo de ℓ-torsión**

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}, \ p \nmid \ell.$$

$$E[p^i] \cong \begin{cases} \mathbb{Z}/p^i\mathbb{Z}, & \forall i \geq 0, \\ \{O\}, & \forall i \geq 0. \end{cases}$$

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)
- Si $E[p]=\{O\}$, decimos que E es una curva supersingular.

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)
- Si $E[p]=\{O\}$, decimos que E es una curva supersingular.
- Todas las curvas supersingulares pueden ser definidas sobre $\mathbb{F}_{p^2}$.

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)
- Si $E[p]=\{O\}$, decimos que E es una curva supersingular.
- Todas las curvas supersingulares pueden ser definidas sobre $\mathbb{F}_{p^2}$.
- Existen $\approx \dfrac{p}{12}$ clases de isomorfismos de curvas supersingulares sobre $\overline{\mathbb{F}}_p$.

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)
- Si $E[p]=\{O\}$, decimos que E es una curva supersingular.
- Todas las curvas supersingulares pueden ser definidas sobre $\mathbb{F}_{p^2}$.
- Existen $\approx \dfrac{p}{12}$ clases de isomorfismos de curvas supersingulares sobre $\overline{\mathbb{F}}_p$.
- Todas las curvas supersingulares sobre $\mathbb{F}_{p^2}$ están en la misma clase de isogenia.

Curvas Supersingulares

- Hay $\ell+1$ subgrupos de $\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}$ de orden ℓ, luego existen $\ell+1$ isogenas de grado ℓ sobre $\overline{\mathbb{F}}_q$ (algunas de ellas podrían no estar definidas sobre $\mathbb{F}_q$.)
- Si $E[p]=\{O\}$, decimos que E es una curva supersingular.
- Todas las curvas supersingulares pueden ser definidas sobre $\mathbb{F}_{p^2}$.
- Existen $\approx \frac{p}{12}$ clases de isomorfismos de curvas supersingulares sobre $\overline{\mathbb{F}}_p$.
- Todas las curvas supersingulares sobre $\mathbb{F}_{p^2}$ están en la misma clase de isogenia.
- Dos curvas son ℓ- isogenas si existe una isogenia de grado ℓ entre ellas.

Supersingular Isogeny Diffie-Hellman (SIDH) [De Feo-Jao 2011 [13]; De Feo-Jao-Plût 2014 [11]]

Parámetros Públicos (E, P_A, Q_A, P_B, Q_B)

- Un primo $p = 2^{e_A}3^{e_B} - 1$, con $2^{e_A} \approx 3^{e_B}$.

Supersingular Isogeny Diffie-Hellman (SIDH) [De Feo-Jao 2011 [13]; De Feo-Jao-Plût 2014 [11]]

Parámetros Públicos (E, P_A, Q_A, P_B, Q_B)

- Un primo $p = 2^{e_A}3^{e_B} - 1$, con $2^{e_A} \approx 3^{e_B}$.
- Curva elíptica supersingular E sobre $\mathbb{F}_{p^2}$ con $|E(\mathbb{F}_{p^2})| = (p+1)^2 = (2^{e_A}3^{e_B})^2$.

Supersingular Isogeny Diffie-Hellman (SIDH) [De Feo-Jao 2011 [13]; De Feo-Jao-Plût 2014 [11]]

Parámetros Públicos (E, P_A, Q_A, P_B, Q_B)

- Un primo $p = 2^{e_A}3^{e_B} - 1$, con $2^{e_A} \approx 3^{e_B}$.
- Curva elíptica supersingular E sobre $\mathbb{F}_{p^2}$ con $|E(\mathbb{F}_{p^2})| = (p+1)^2 = (2^{e_A}3^{e_B})^2$.
- Puntos P_A, Q_A, P_B, Q_B en la curva generando los subgrupos de torsión:

Supersingular Isogeny Diffie-Hellman (SIDH) [De Feo-Jao 2011 [13]; De Feo-Jao-Plût 2014 [11]]

Parámetros Públicos (E, P_A, Q_A, P_B, Q_B)

- Un primo $p = 2^{e_A}3^{e_B} - 1$, con $2^{e_A} \approx 3^{e_B}$.
- Curva elíptica supersingular E sobre $\mathbb{F}_{p^2}$ con $|E(\mathbb{F}_{p^2})| = (p+1)^2 = (2^{e_A}3^{e_B})^2$.
- Puntos P_A, Q_A, P_B, Q_B en la curva generando los subgrupos de torsión:

Supersingular Isogeny Diffie-Hellman (SIDH) [De Feo-Jao 2011 [13]; De Feo-Jao-Plût 2014 [11]]

Parámetros Públicos (E, P_A, Q_A, P_B, Q_B)

- Un primo $p = 2^{e_A}3^{e_B} - 1$, con $2^{e_A} \approx 3^{e_B}$.
- Curva elíptica supersingular E sobre $\mathbb{F}_{p^2}$ con $|E(\mathbb{F}_{p^2})| = (p+1)^2 = (2^{e_A}3^{e_B})^2$.
- Puntos P_A, Q_A, P_B, Q_B en la curva generando los subgrupos de torsión:

$$\langle P_A, Q_A \rangle = E[2^{e_A}]$$

$$\langle P_B, Q_B \rangle = E[3^{e_B}].$$

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
- Análogamente, Bob escoge un número aleatorio $n_B \in \mathbb{Z}/3^{e_A}\mathbb{Z}$ y calcula:

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
- Análogamente, Bob escoge un número aleatorio $n_B \in \mathbb{Z}/3^{e_A}\mathbb{Z}$ y calcula:

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
- Análogamente, Bob escoge un número aleatorio $n_B \in \mathbb{Z}/3^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle B \rangle = \langle P_B + [n_B]Q_B \rangle$.

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
- Análogamente, Bob escoge un número aleatorio $n_B \in \mathbb{Z}/3^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle B \rangle = \langle P_B + [n_B]Q_B \rangle$.
  Isogenia secreta: $\phi_B : E \to E_B = E/\langle B \rangle$, con $\ker\phi_B = \langle B \rangle$.

SIDH

Generación de Claves

- Alice escoge un número aleatorio $n_A \in \mathbb{Z}/2^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle A \rangle = \langle P_A + [n_A]Q_A \rangle$
  Isogenia secreta: $\phi_A : E \to E_A = E/\langle A \rangle$, con $\ker\phi_A = \langle A \rangle$.
  Clave secreta: n_A. **Clave pública**: $(E_A, \phi_A(P_B), \phi_A(Q_B))$.
- Análogamente, Bob escoge un número aleatorio $n_B \in \mathbb{Z}/3^{e_A}\mathbb{Z}$ y calcula:
  Subgrupo secreto: $\langle B \rangle = \langle P_B + [n_B]Q_B \rangle$.
  Isogenia secreta: $\phi_B : E \to E_B = E/\langle B \rangle$, con $\ker\phi_B = \langle B \rangle$.
  Clave secreta: n_B. **Clave pública**: $(E_B, \phi_B(P_A), \phi_B(Q_A))$.

SIDH

Secreto Compartido

- Alice calcula $\phi_B(A)$:

$$\phi_B(A) = \phi_B(P_A + [n_A]Q_A) = \phi_B(P_A) + [n_A]\phi_B(Q_A)$$

y la isogenia $\psi_A : E_B \to E_B/\langle \phi_B(A) \rangle := E_{AB}$.

SIDH

Secreto Compartido

- Alice calcula $\phi_B(A)$:

$$\phi_B(A) = \phi_B(P_A + [n_A]Q_A) = \phi_B(P_A) + [n_A]\phi_B(Q_A)$$

y la isogenia $\psi_A : E_B \to E_B/\langle \phi_B(A) \rangle := E_{AB}$.

- Análogamente, Bob calcula:

$$\phi_A(B) = \phi_A(P_B + [n_B]Q_B) = \phi_A(P_B) + [n_B]\phi_A(Q_B)$$

y la isogenia $\psi_B : E_A \to E_A/\langle \phi_A(B) \rangle := E_{BA}$.

SIDH

Secreto Compartido

- Alice calcula $\phi_B(A)$:

$$\phi_B(A) = \phi_B(P_A + [n_A]Q_A) = \phi_B(P_A) + [n_A]\phi_B(Q_A)$$

  y la isogenia $\psi_A : E_B \to E_B/\langle \phi_B(A) \rangle := E_{AB}$.

- Análogamente, Bob calcula:

$$\phi_A(B) = \phi_A(P_B + [n_B]Q_B) = \phi_A(P_B) + [n_B]\phi_A(Q_B)$$

  y la isogenia $\psi_B : E_A \to E_A/\langle \phi_A(B) \rangle := E_{BA}$.

- E_{AB} y E_{BA} son isomorfas a la curva $E/\langle A, B \rangle$.

SIDH

Secreto Compartido

- Alice calcula $\phi_B(A)$:

$$\phi_B(A) = \phi_B(P_A + [n_A]Q_A) = \phi_B(P_A) + [n_A]\phi_B(Q_A)$$

  y la isogenia $\psi_A : E_B \to E_B/\langle \phi_B(A) \rangle := E_{AB}$.

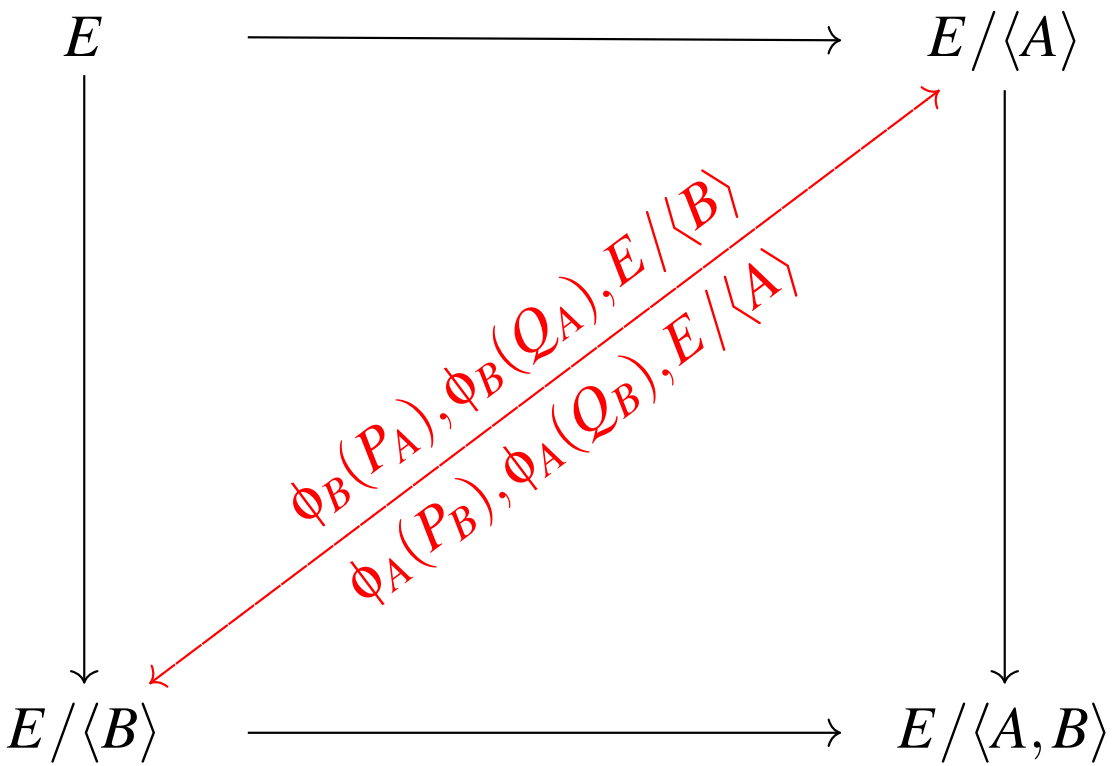
- Análogamente, Bob calcula:

$$\phi_A(B) = \phi_A(P_B + [n_B]Q_B) = \phi_A(P_B) + [n_B]\phi_A(Q_B)$$

  y la isogenia $\psi_B : E_A \to E_A/\langle \phi_A(B) \rangle := E_{BA}$.

- E_{AB} y E_{BA} son isomorfas a la curva $E/\langle A, B \rangle$.
- **Secreto compartido**: $j(E_{AB}) = j(E_{BA})$.

SIDH


E
$E/\langle A \rangle$
$E/\langle B \rangle$
$E/\langle A, B \rangle$
$\phi_B(P_A), \phi_B(Q_A), E/\langle B \rangle$
$\phi_A(P_B), \phi_A(Q_B), E/\langle A \rangle$

SIDH

Seguridad de SIDH : Supersingular isogeny problem: Dados los parámetros públicos $e_A, e_B, p, E, E_A, P_A, Q_A, P_B, Q_B$ y $\phi_A(P_B), \phi_A(Q_B)$, calcular la isogenia de grado 2^{e_A}, $\phi_A : E \to E_A$,

SIDH

Seguridad de SIDH : Supersingular isogeny problem: Dados los parámetros públicos $e_A, e_B, p, E, E_A, P_A, Q_A, P_B, Q_B$ y $\phi_A(P_B), \phi_A(Q_B)$, calcular la isogenia de grado 2^{e_A}, $\phi_A : E \to E_A$,

Aspectos computacionales:

- Aritmética en $\mathbb{F}_p$: adición, multiplicación, inversión.
- Aritmética en $\mathbb{F}_{p^2}$: adición, multiplicación, cuadrados, inversión.
- Aritmética de la curva: adición de puntos, doblado, evaluación de isogenias en puntos.
- Aritmética de extendida de la curva: $P + [k]Q$, cálculo de isogenias de grado grande.
- Protocolos: SIDH

SIDH

Seguridad de SIDH : Supersingular isogeny problem: Dados los parámetros públicos $e_A, e_B, p, E, E_A, P_A, Q_A, P_B, Q_B$ y $\phi_A(P_B), \phi_A(Q_B)$, calcular la isogenia de grado 2^{e_A}, $\phi_A : E \to E_A$,

Aspectos computacionales:

- Aritmética en $\mathbb{F}_p$: adición, multiplicación, inversión.
- Aritmética en $\mathbb{F}_{p^2}$: adición, multiplicación, cuadrados, inversión.
- Aritmética de la curva: adición de puntos, doblado, evaluación de isogenias en puntos.
- Aritmética de extendida de la curva: $P + [k]Q$, cálculo de isogenias de grado grande.
- Protocolos: SIDH

Mas detalles de SIDH en : [10], [4], [13], [12].

Cálculo efectivo de isogenias

Fórmulas de Vélu [20]

Dada una curva elíptica E/K y un subgrupo finito G de $E(K)$, podemos obtener una curva $E' = E/G$ y una isogenia separable $\phi : E \to E'$ con $\ker \phi = G$.

Cálculo efectivo de isogenias

Fórmulas de Vélu [20]

Dada una curva elíptica E/K y un subgrupo finito G de $E(K)$, podemos obtener una curva $E' = E/G$ y una isogenia separable $\phi : E \to E'$ con $\ker \phi = G$.

Mas precisamente, si $|G| = \ell$, entonces

Cálculo efectivo de isogenias

Fórmulas de Vélu [20]

Dada una curva elíptica E/K y un subgrupo finito G de $E(K)$, podemos obtener una curva $E' = E/G$ y una isogenia separable $\phi : E \to E'$ con $\ker \phi = G$.

Mas precisamente, si $|G| = \ell$, entonces

$$\phi(x,y) = \left(\frac{g(x)}{h(x)}, y \left(\frac{g(x)}{h(x)} \right)' \right),$$

donde $h(x) = \prod_{Q \in G^*} (x - x(Q))$ y deg($h(x)$)=$\ell - 1$.

Fórmulas de Vélu

Si σ es la suma de las abscisas de los puntos en G^*, entonces:

$$\frac{g(x)}{h(x)} = \ell x - \sigma - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)',$$

con $h(x) = x^{\ell-1} - \sigma x^{l-2} + \cdots$ y $y^2 = f(x)$.

Fórmulas de Vélu

Si σ es la suma de las abscisas de los puntos en G^*, entonces:

$$\frac{g(x)}{h(x)} = \ell x - \sigma - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)',$$

con $h(x) = x^{\ell-1} - \sigma x^{l-2} + \cdots$ y $y^2 = f(x)$.
Si $t = \sum_{Q \in G^*} f'(Q), u = \sum_{Q \in G^*} 2f(Q)$ y $w = u + \sum_{Q \in G^*} x(Q)f'(Q)$, entonces

$$E' : y^2 = x^3 + a_2x^2 + (a_4 - 5t)x + a_6 - 4a_2t - 7w.$$

Fórmulas de Vélu

Si σ es la suma de las abscisas de los puntos en G^*, entonces:

$$\frac{g(x)}{h(x)} = \ell x - \sigma - f'(x)\frac{h'(x)}{h(x)} - 2f(x)\left(\frac{h'(x)}{h(x)}\right)',$$

con $h(x) = x^{\ell-1} - \sigma x^{l-2} + \cdots$ y $y^2 = f(x)$.
Si $t = \sum_{Q \in G^*} f'(Q), u = \sum_{Q \in G^*} 2f(Q)$ y $w = u + \sum_{Q \in G^*} x(Q)f'(Q)$, entonces

$$E' : y^2 = x^3 + a_2x^2 + (a_4 - 5t)x + a_6 - 4a_2t - 7w.$$

Fórmulas de Vélu tienen costo polinomial en $|G|$ y $\log p$.

Estrategias para calcular ℓ^e-isogenias

Descomponer ϕ como una cadena de ℓ-isogenias:

Estrategias para calcular ℓ^e-isogenias

Descomponer ϕ como una cadena de ℓ-isogenias:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \cdots \qquad E_{e-1} \xrightarrow{\phi_{e-1}} E_e$$

donde, R es un punto de orden ℓ^e, $E_0 = E$,

$$E_{i+1} = E_i / \langle \ell^{e-i-1} R_i \rangle$$

$$\phi_i : E_i \to E_{i+1}$$

$$R_{i+1} = \phi(R_i)$$

y $E/\langle R \rangle = E_e$.

Curvas de Montgomery

Curvas de Montgomery están dadas por la ecuación afín

$$E_{a,b} : by^2 = x^3 + ax^2 + x$$

donde $a, b \in \mathbb{F}_q$ satisfacen $b(a^2 - 4) \neq 0$. Versión proyectiva:

$$E_{a,b} : bY^2Z = X(X^2 + aXZ + Z^2) \subseteq \mathbb{P}^2$$

y $O = (0 : 1 : 0)$ es el único punto en el infinito.

Curvas de Montgomery

Curvas de Montgomery están dadas por la ecuación afín

$$E_{a,b} : by^2 = x^3 + ax^2 + x$$

donde $a, b \in \mathbb{F}_q$ satisfacen $b(a^2 - 4) \neq 0$. Versión proyectiva:

$$E_{a,b} : bY^2Z = X(X^2 + aXZ + Z^2) \subseteq \mathbb{P}^2$$

y $O = (0 : 1 : 0)$ es el único punto en el infinito.
El inverso de $(x : y : 1)$ is $(x : -y : 1)$.

Curvas de Montgomery

Curvas de Montgomery están dadas por la ecuación afín

$$E_{a,b} : by^2 = x^3 + ax^2 + x$$

donde $a, b \in \mathbb{F}_q$ satisfacen $b(a^2 - 4) \neq 0$. Versión proyectiva:

$$E_{a,b} : bY^2Z = X(X^2 + aXZ + Z^2) \subseteq \mathbb{P}^2$$

y $O = (0 : 1 : 0)$ es el único punto en el infinito.
El inverso de $(x : y : 1)$ is $(x : -y : 1)$.
Una curva de Montgomery puede ser transformada a una curva de Weiestrass. El recíproco en general no es válido.

Curvas de Montgomery

Ventajas de este modelo: aritmética diferencial rápida

Curvas de Montgomery

Ventajas de este modelo: aritmética diferencial rápida

Si $P \neq Q$ y diferente a $O, T = (0:0:1)$, existe una relación entre x_P, x_Q, x_{P+Q} y x_{P-Q}:

$$x_{P+Q}x_{P-Q}(x_P - x_Q)^2 = (x_P x_Q - 1)^2,$$

Curvas de Montgomery

Ventajas de este modelo: aritmética diferencial rápida

Si $P \neq Q$ y diferente a $O, T = (0:0:1)$, existe una relación entre x_P, x_Q, x_{P+Q} y x_{P-Q}:

$$x_{P+Q}x_{P-Q}(x_P - x_Q)^2 = (x_P x_Q - 1)^2,$$

Si $P = Q$ y $[2]P = (x_{[2]P}, y_{[2]P})$, entonces

$$4x_{[2]P}x_P(x_P^2 + Ax_P + 1) = (x_P^2 - 1)^2.$$

Aritmética de la Curva

- Para calcular $[k]P$: escalera de Montgomery (1987, P. Montgomery [16], [6]).

Aritmética de la Curva

- Para calcular $[k]P$: escalera de Montgomery (1987, P. Montgomery [16], [6]).
- Para calcular $P + [k]Q$: escalera de tres puntos (2018, Faz-Hernández–López–Ochoa-Jiménez–Rodríguez-Henríquez [9]).

Aritmética de la Curva

- Para calcular $[k]P$: escalera de Montgomery (1987, P. Montgomery [16], [6]).
- Para calcular $P + [k]Q$: escalera de tres puntos (2018, Faz-Hernández–López–Ochoa-Jiménez–Rodríguez-Henríquez [9]).
- Aritmética menos costosa (en términos de operaciones en $\mathbb{F}_p$) que en modelo de Weierstrass.

2-Isogenias en curvas de Montgomery

Considerar al punto de orden 2, $P = (0,0)$.

- El twist $\mu : E_{a,b} \to E_0$ dado por $(x,y) = (x, \sqrt{b}y)$ lleva $E_{a,b} : by^2 = x^3 + ax^2 + x$ en $E_0 : y^2 = x^3 + ax^2 + x$.

2-Isogenias en curvas de Montgomery

Considerar al punto de orden 2, $P = (0,0)$.

- El twist $\mu : E_{a,b} \to E_0$ dado por $(x,y) = (x, \sqrt{b}y)$ lleva $E_{a,b} : by^2 = x^3 + ax^2 + x$ en $E_0 : y^2 = x^3 + ax^2 + x$.
- Aplicamos las fórmulas de Vélu a E_0.

2-Isogenias en curvas de Montgomery

Considerar al punto de orden 2, $P = (0,0)$.

- El twist $\mu : E_{a,b} \to E_0$ dado por $(x,y) = (x, \sqrt{b}y)$ lleva $E_{a,b} : by^2 = x^3 + ax^2 + x$ en $E_0 : y^2 = x^3 + ax^2 + x$.
- Aplicamos las fórmulas de Vélu a E_0.
- Componemos con el twist:

$$\phi : \quad E_{a,b} \to \quad E_1 : by^2 = x^3 + (a+6)x^2 + 4(a+2)x$$

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

2-Isogenias en curvas de Montgomery

Considerar al punto de orden 2, $P = (0,0)$.

- El twist $\mu : E_{a,b} \to E_0$ dado por $(x,y) = (x, \sqrt{b}y)$ lleva $E_{a,b} : by^2 = x^3 + ax^2 + x$ en $E_0 : y^2 = x^3 + ax^2 + x$.
- Aplicamos las fórmulas de Vélu a E_0.
- Componemos con el twist:

$$\phi : \quad E_{a,b} \to \quad E_1 : by^2 = x^3 + (a+6)x^2 + 4(a+2)x$$

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

- E_1 no es una curva de Montgomery. Transformaciones requieren raíces cuadradas!

4-Isogenias

Solución: calcular 4-isogenias

- Considerar la 2-isogenia $\tau : E_1 \to E_2 = E_1/\langle (0,0) \rangle$ dada por

$$\tau(x,y) = \left(\frac{1}{2-a} \frac{(x+4)(x+(a+2))}{x}, \frac{y}{2-a}\left(1 - \frac{4(2+a)}{x^2}\right)\right),$$

y con E_2 : $\quad \dfrac{b}{2-a}\, y^2 = x^3 - 2\dfrac{a+6}{2-a} + x.$

4-Isogenias

Solución: calcular 4-isogenias

- Considerar la 2-isogenia $\tau : E_1 \to E_2 = E_1/\langle (0,0) \rangle$ dada por

$$\tau(x,y) = \left(\frac{1}{2-a} \frac{(x+4)(x+(a+2))}{x}, \frac{y}{2-a}\left(1 - \frac{4(2+a)}{x^2}\right)\right),$$

  y con E_2 : $\dfrac{b}{2-a}\, y^2 = x^3 - 2\dfrac{a+6}{2-a} + x.$

- Considerar $\phi_4 = \tau \circ \phi$. Necesitamos evitar la isogenia dual de ϕ_4 en el siguiente paso, luego necesitamos combinar con un isomorfismo.

4-Isogenias

Solución: calcular 4-isogenias

- Considerar la 2-isogenia $\tau : E_1 \to E_2 = E_1/\langle(0,0)\rangle$ dada por

$$\tau(x,y) = \left(\frac{1}{2-a}\frac{(x+4)(x+(a+2))}{x}, \frac{y}{2-a}\left(1-\frac{4(2+a)}{x^2}\right)\right),$$

  y con E_2 : $\dfrac{b}{2-a}\,y^2 = x^3 - 2\dfrac{a+6}{2-a} + x.$

- Considerar $\phi_4 = \tau \circ \phi$. Necesitamos evitar la isogenia dual de ϕ_4 en el siguiente paso, luego necesitamos combinar con un isomorfismo.
- En 2017, Renes [17] obtiene una fórmula para calcular 2-isogenias evitando raíces cuadradas, con $P \neq (0,0)$.

4-Isogenias

Solución: calcular 4-isogenias

- Considerar la 2-isogenia $\tau : E_1 \to E_2 = E_1/\langle(0,0)\rangle$ dada por

$$\tau(x,y) = \left(\frac{1}{2-a}\frac{(x+4)(x+(a+2))}{x}, \frac{y}{2-a}\left(1-\frac{4(2+a)}{x^2}\right)\right),$$

  y con E_2 : $\dfrac{b}{2-a}\,y^2 = x^3 - 2\dfrac{a+6}{2-a} + x.$

- Considerar $\phi_4 = \tau \circ \phi$. Necesitamos evitar la isogenia dual de ϕ_4 en el siguiente paso, luego necesitamos combinar con un isomorfismo.
- En 2017, Renes [17] obtiene una fórmula para calcular 2-isogenias evitando raíces cuadradas, con $P \neq (0,0)$.
- En 2016, Costello, Longa y Naehrig [5] realizaron implementaciones para SIDH considerando la curva $y^2 : x^3 + x$ y ahora $y^2 = x^3 + 6x^2 + x$.

Preguntas

- Curvas de Edwards (twisted) $ax^2 + y^2 = 1 + dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.

Preguntas

- Curvas de Edwards (twisted) $ax^2 + y^2 = 1 + dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:

Preguntas

- Curvas de Edwards (twisted) $ax^2 + y^2 = 1 + dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:

Preguntas

- Curvas de Edwards (twisted) $ax^2 + y^2 = 1 + dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:
  Curvas de Huff: $x(ay^2 - 1) = y(bx^2 - 1)$, con $ab(a - b) \neq 0$.

Preguntas

- Curvas de Edwards (twisted) $ax^2 + y^2 = 1 + dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:
  Curvas de Huff: $x(ay^2 - 1) = y(bx^2 - 1)$, con $ab(a - b) \neq 0$.
  Curvas Hessian : $ax^3 + y^3 + 1 = dxy$, con $d^3 \neq 27$ y $a(27a - d^3) \neq 0$.

Preguntas

- Curvas de Edwards (twisted) $ax^2+y^2=1+dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:
  Curvas de Huff: $x(ay^2-1)=y(bx^2-1)$, con $ab(a-b)\neq 0$.
  Curvas Hessian : $ax^3+y^3+1=dxy$, con $d^3\neq 27$ y $a(27a-d^3)\neq 0$.
  Intersección de Jacobi:

$$J_a:\left\{\begin{array}{rcl} x^2+y^2 & = & 1, \\ ax^2+z^2 & = & 1, \end{array}\right.$$

  con $a(1-a)\neq 0$.

Preguntas

- Curvas de Edwards (twisted) $ax^2+y^2=1+dx^2y^2$ son birracionalmente equivalentes a curvas de Montgomery. De aqui en 2018, Kim, Yoon et al [14], obtuvieron fórmulas eficientes para calcular isogenias. Se probó que son competitivas con Montgomery.
- Otros modelos:
  Curvas de Huff: $x(ay^2-1)=y(bx^2-1)$, con $ab(a-b)\neq 0$.
  Curvas Hessian : $ax^3+y^3+1=dxy$, con $d^3\neq 27$ y $a(27a-d^3)\neq 0$.
  Intersección de Jacobi:

$$J_a:\left\{\begin{array}{rcl} x^2+y^2 & = & 1, \\ ax^2+z^2 & = & 1, \end{array}\right.$$

  con $a(1-a)\neq 0$.

Commutative Supersingular Isogeny Diffie-Hellman: CSIDH [Castryck, Lange, Martindale, Rennes (2018) [2]]

Sea E una curva elíptica definida sobre $\mathbb{F}_p$.

- $End_p(E) = \{\alpha \in End(E) :\ \alpha$ está definido sobre $\mathbb{F}_p\}$.

Commutative Supersingular Isogeny Diffie-Hellman: CSIDH [Castryck, Lange, Martindale, Rennes (2018) [2]]

Sea E una curva elíptica definida sobre $\mathbb{F}_p$.

- $End_p(E) = \{\alpha \in End(E) : \ \alpha$ está definido sobre $\mathbb{F}_p\}$.
- $End_p(E)$ es isomorfo a un orden en el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{t_p^2 - 4p})$, donde t_p es la traza de Frobenius.

Commutative Supersingular Isogeny Diffie-Hellman: CSIDH [Castryck, Lange, Martindale, Rennes (2018) [2]]

Sea E una curva elíptica definida sobre $\mathbb{F}_p$.

- $End_p(E) = \{\alpha \in End(E) : \ \alpha$ está definido sobre $\mathbb{F}_p\}$.
- $End_p(E)$ es isomorfo a un orden en el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{t_p^2 - 4p})$, donde t_p es la traza de Frobenius.
- Si $E/\mathbb{F}_p$ es supersingular, $t = 0$

Commutative Supersingular Isogeny Diffie-Hellman: CSIDH [Castryck, Lange, Martindale, Rennes (2018) [2]]

Sea E una curva elíptica definida sobre $\mathbb{F}_p$.

- $End_p(E) = \{\alpha \in End(E) : \ \alpha$ está definido sobre $\mathbb{F}_p\}$.
- $End_p(E)$ es isomorfo a un orden en el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{t_p^2 - 4p})$, donde t_p es la traza de Frobenius.
- Si $E/\mathbb{F}_p$ es supersingular, $t = 0$
- Denotamos por $\mathcal{E}\ell\ell_p(O)$, al conjunto de curvas elípticas E/F_p tales que $End_p(E) \cong O$

Commutative Supersingular Isogeny Diffie-Hellman: CSIDH [Castryck, Lange, Martindale, Rennes (2018) [2]]

Sea E una curva elíptica definida sobre $\mathbb{F}_p$.

- $End_p(E) = \{\alpha \in End(E) : \ \alpha$ está definido sobre $\mathbb{F}_p\}$.
- $End_p(E)$ es isomorfo a un orden en el cuerpo cuadrático imaginario $\mathbb{Q}(\sqrt{t_p^2 - 4p})$, donde t_p es la traza de Frobenius.
- Si $E/\mathbb{F}_p$ es supersingular, $t = 0$
- Denotamos por $\mathcal{E}\ell\ell_p(O)$, al conjunto de curvas elípticas E/F_p tales que $End_p(E) \cong O$
- Si $[\mathfrak{a}]$ es una clase de ideales en Cl(O), se tiene que $E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$.

  es un subgrupo finito de $E(\mathbb{F}_p)$.

CSIDH

$$\begin{array}{ccc} \mathrm{Cl}(O) \times \mathcal{E}\ell\ell_p(O) & \longrightarrow & \mathcal{E}\ell\ell_p(O) \\ ([\mathfrak{a}], E) & \longmapsto & [\mathfrak{a}] * E := E/E[\mathfrak{a}] \end{array}$$

es una acción fiel y transitiva.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Parametros Públicos:

- Primos impares pequeños ℓ_i tales que $p = 4\prod_{i=1}^{n} \ell_i - 1$ es primo.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Parametros Públicos:

- Primos impares pequeños ℓ_i tales que $p = 4\prod_{i=1}^{n} \ell_i - 1$ es primo.
- Curva de Montogomery supersingular definida sobre $\mathbb{F}_p$, $E_A : y^2 = x^3 + Ax^2 + x$, con $\#E(\mathbb{F}_p) = p + 1$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Parametros Públicos:

- Primos impares pequeños ℓ_i tales que $p = 4\prod_{i=1}^{n} \ell_i - 1$ es primo.
- Curva de Montogomery supersingular definida sobre $\mathbb{F}_p$, $E_A : y^2 = x^3 + Ax^2 + x$, con $\#E(\mathbb{F}_p) = p + 1$.
- Observación: Si $p \equiv 3 \mod 8$ y $E/\mathbb{F}_p$ es supersingular, entonces

$$End_p(E) \cong \mathbb{Z}[\sqrt{-p}]$$

si y solo si, $E \cong E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$, donde $A \in \mathbb{F}_p$ es único.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Parametros Públicos:

- Primos impares pequeños ℓ_i tales que $p = 4\prod_{i=1}^{n} \ell_i - 1$ es primo.
- Curva de Montogomery supersingular definida sobre $\mathbb{F}_p$, $E_A : y^2 = x^3 + Ax^2 + x$, con $\#E(\mathbb{F}_p) = p + 1$.
- Observación: Si $p \equiv 3 \mod 8$ y $E/\mathbb{F}_p$ es supersingular, entonces

$$End_p(E) \cong \mathbb{Z}[\sqrt{-p}]$$

si y solo si, $E \cong E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$, donde $A \in \mathbb{F}_p$ es único.

- Como los primos $\ell_i \mid p + 1$, entonces el ideal primo (ℓ_i) de $\mathbb{Z}[\sqrt{-p}]$ se factoriza como $(\ell_i, \sqrt{-p} - 1)(\ell_i, \sqrt{-p} + 1)$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Generación de Claves

- Alice:

clave privada:$(a_1, .., a_n) \in \{-m, ..., m\}^n \to \mathfrak{a} = \mathfrak{l}_1^{a_1} \cdot \mathfrak{l}_2^{a_2} \cdots \mathfrak{l}_n^{a_n}$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Generación de Claves

- Alice:

clave privada:$(a_1, .., a_n) \in \{-m, ..., m\}^n \to \mathfrak{a} = \mathfrak{l}_1^{a_1} \cdot \mathfrak{l}_2^{a_2} \cdots \mathfrak{l}_n^{a_n}$.

clave pública: $[\mathfrak{a}] * E_A$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Generación de Claves

- Alice:

clave privada:$(a_1,..,a_n) \in \{-m,...,m\}^n \to \mathfrak{a} = \mathfrak{l}_1^{a_1} \cdot \mathfrak{l}_2^{a_2} \cdots \mathfrak{l}_n^{a_n}$.

clave pública: $[\mathfrak{a}] * E_A$.

- Bob:

clave privada $(b_1,..,b_n) \in \{-m,...,m\}^n \to \mathfrak{b} = \mathfrak{l}_1^{b_1} \cdot \mathfrak{l}_2^{b_2} \cdots \mathfrak{l}_n^{b_n}$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Generación de Claves

- Alice:

clave privada:$(a_1,..,a_n) \in \{-m,...,m\}^n \to \mathfrak{a} = \mathfrak{l}_1^{a_1} \cdot \mathfrak{l}_2^{a_2} \cdots \mathfrak{l}_n^{a_n}$.

clave pública: $[\mathfrak{a}] * E_A$.

- Bob:

clave privada $(b_1,..,b_n) \in \{-m,...,m\}^n \to \mathfrak{b} = \mathfrak{l}_1^{b_1} \cdot \mathfrak{l}_2^{b_2} \cdots \mathfrak{l}_n^{b_n}$.

clave pública: $[\mathfrak{b}] * E_A$.

CSIDH: Commutative Supersingular Isogeny Diffie-Hellman

Generación de Claves

- Alice:

clave privada:$(a_1,..,a_n) \in \{-m,...,m\}^n \to \mathfrak{a} = \mathfrak{l}_1^{a_1} \cdot \mathfrak{l}_2^{a_2} \cdots \mathfrak{l}_n^{a_n}$.
clave pública: $[\mathfrak{a}] * E_A$.

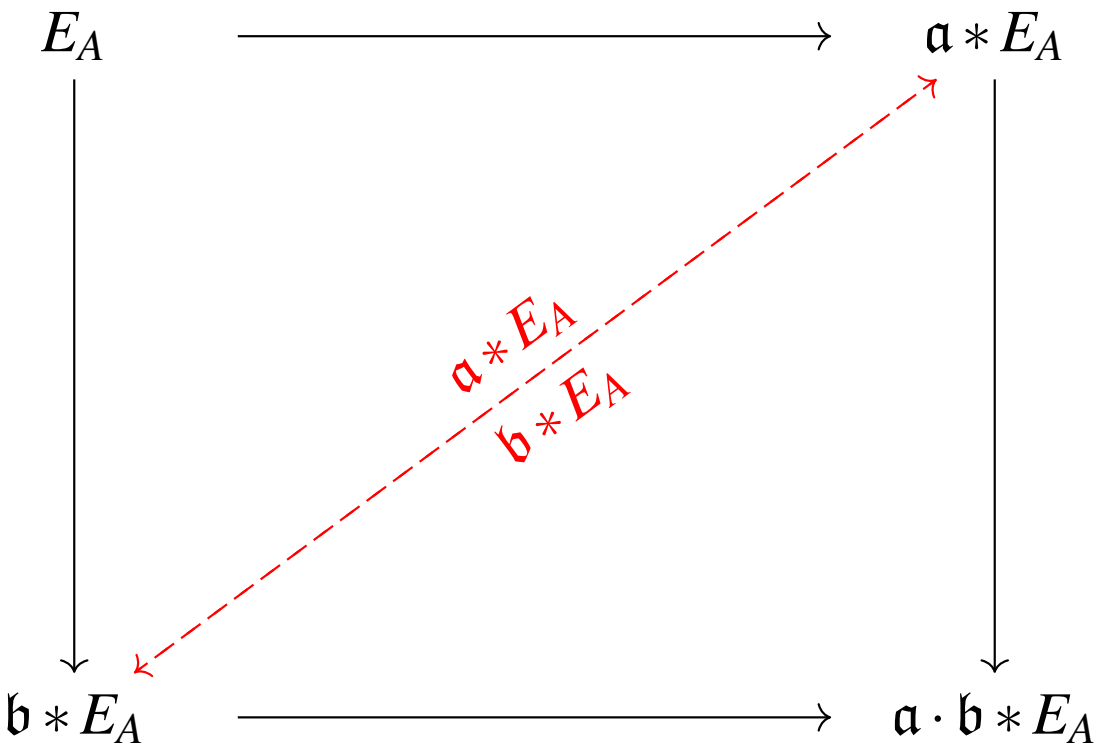
- Bob:

clave privada $(b_1,..,b_n) \in \{-m,...,m\}^n \to \mathfrak{b} = \mathfrak{l}_1^{b_1} \cdot \mathfrak{l}_2^{b_2} \cdots \mathfrak{l}_n^{b_n}$.
clave pública: $[\mathfrak{b}] * E_A$.

Secreto Compartido

$$[\mathfrak{a}] * ([\mathfrak{b}] * E_A) = [\mathfrak{b}] * ([\mathfrak{a}] * E_A) = [\mathfrak{a} \cdot \mathfrak{b}] * E_A$$

CSIDH


E_A
$\mathfrak{a} * E_A$
$\mathfrak{a} * E_A$
$\mathfrak{b} * E_A$
$\mathfrak{b} * E_A$
$\mathfrak{a} \cdot \mathfrak{b} * E_A$

CSIDH

Seguridad: Dadas E y E' curvas supersingulares sobre $\mathbb{F}_p$ tales que $End_p(E) \cong End_p(E')$, determinar un ideal $\mathfrak{a}$ tal que $[\mathfrak{a}] * E = E'$.

CSIDH

Seguridad: Dadas E y E' curvas supersingulares sobre $\mathbb{F}_p$ tales que $End_p(E) \cong End_p(E')$, determinar un ideal $\mathfrak{a}$ tal que $[\mathfrak{a}] * E = E'$.

Observación:

- Si $\mathfrak{l}_i = (\ell_i, \pi - 1)$, entonces $\ker \rho_{\mathfrak{l}_i} = \langle P \rangle$, con $P \in E(\mathbb{F}_p)$ de orden ℓ_i.
- Si $\bar{\mathfrak{l}}_i = (\ell_i, \pi - 1)$, entonces $\ker \rho_{\bar{\mathfrak{l}}_i} = \langle P \rangle$, con $P = (x, iy) \in E(\mathbb{F}_p^2)$ de orden ℓ_i, con $x, y \in \mathbb{F}_p$, $i = \sqrt{-1}$, $i^p = -i$.

Problemas

- En 2018 Castryck y Decru [1] consideraron para $p \equiv 3$ mod 4 curvas supersingulares con $End_p(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$: "CSIDH on the surface" (CSURF).

Problemas

- En 2018 Castryck y Decru [1] consideraron para $p \equiv 3$ mod 4 curvas supersingulares con $End_p(E) \cong \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$: "CSIDH on the surface" (CSURF).
- ¿ Otros modelos de curvas?

Publicidad!

Escuela CIMPA: Isogenies of elliptic curves and their applications to cryptography

`www.rnta.eu/Popayan2021`

Universidad del Cauca, Popayán, Colombia, Julio 19-30, 2021

Cursos:

Algebraic Number Theory (Yuri Bilu and Amalia Pizarro)

Graph Theory (Amanda Montejano and Carlos Trujillo)

Finite fields (Florian Luca and Michel Waldschmidt)

Elliptic curves over finite fields (Francesco Pappalardi and Valerio Talamanca)

Elliptic curves (Gonzalo Tornaría and Cecilia Salgado)

Isogenies of elliptic curves (Sorina Ionica and Marusia Rebolledo)

Isogeny Based Cryptography (Luca De Feo and Julio Lopez)

- Wouter Castryck and Thomas Decru, *Csidh on the surface*, PQCrypto 2020, Paris, France, April 15-17, Proceedings, Springer, 2020, https://eprint.iacr.org/2019/1404.
- Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes, *Csidh: An efficient post-quantum commutative group action*, 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III, 2018, https://eprint.iacr.org/2018/383.
- Denis Charles, Eyal Goren, and Kristin Lauter, *Cryptographic hash functions from expander graphs*, Cryptology ePrint Archive, Report 2006/021, 2006, https://eprint.iacr.org/2006/021.
- Craig Costello and Huseyin Hisil, *A simple and compact algorithm for sidh with arbitrary degree isogenies*, Springer International Publishing, pp. 303–329, 2017, https://eprint.iacr.org/2017/504.
- Craig Costello, David Jao, Patrick Longa, Michael Naehrig, Joost Renes, and David Urbanik, *Efficient compression of sidh public keys*, IACR Cryptology ePrint Archive **2016** (2016), 963.

- Craig Costello and Benjamin Smith, *Montgomery curves and their arithmetic*, 2017.
- Jean-Marc Couveignes, *Hard homogeneous spaces*, IACR Cryptology ePrint Archive, pp. 291, 2006, https://eprint.iacr.org/2006/291.
- Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), no. 6, 644–654 https://doi.org/10.1109/TIT.1976.1055638.
- Armando Faz-Hernández, Julio López, Eduardo Ochoa-Jiménez, and Francisco Rodríguez-Henríquez, *A Faster Software Implementation of the Supersingular Isogeny Diffie-Hellman Key Exchange Protocol*, (2017), https://eprint.iacr.org/2017/1015.
- Luca De Feo, *Mathematics of isogeny based cryptography*, CoRR **abs/1711.04062** (2017).
- Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Mathematical

Cryptology **8** (2014), no. 3, 209–247, https://doi.org/10.1515/jmc\g2012\g0015.

David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik, *Supersingular isogeny key encapsulation*, Submission to Round 2 of NIST's Post-Quantum Cryptography Standardization Process, 2019, 04 2019, https://sike.org.

David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings (Bo-Yin Yang, ed.), Lecture Notes in Computer Science, vol. 7071, Springer, 2011, pp. 19–34, https://eprint.iacr.org/2011/506.

Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong, and Young-Ho Park, *Efficient isogeny computations on twisted edwards curves*, Security

and Communication Networks **2018** (2018), 5747642:1–5747642:11, https://doi.org/10.1155/2018/5747642.


National Institute of Standards and Technology, *Announcing request for nominations for public-key post-quantum cryptographic algorithms*, Tech. report, 2016, https://www.federalregister.gov/d/2016-30615.


Montgomery Peter L., *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264, https://doi.org/10.2307/2007888.


Joost Renes, *Computing isogenies between montgomery curves using the action of (0, 0)*, Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings, 2018, pp. 229–247, https://doi.org/10.1007/978\g3\g319\g79063\g3_11.


Alexander Rostovtsev and Anton Stolbunov, *Public-key cryptosystem based on isogenies*, IACR Cryptology ePrint Archive, 2006, https://eprint.iacr.org/2006/145, p. 145.

Peter W. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), 124–134, https://doi.org/10.1109/SFCS.1994.365700.

Jacques. Vélu, *Isogénies entre courbes elliptiques*, Comptes-Rendus de l'Académie des Sciences, Série I **273** (1971), 238–241.