Криптосистеми на еліптичних кривих

Lecture 11: Isogenies

Грубіян Євген Олександрович

Поняття ізогенії

Definition

Нехай E_1 та E_2 - еліптичні криві над полем K. Ізогенія $\phi : E_1 \to E_2$ - це скінченний морфізм кривих, що є також груповим гомоморфізмом, тобто $\phi(P + Q) = \phi(P) + \phi(Q)$ для всіх $P, Q \in E_1(\bar{K})$

- Якщо ϕ не нульовий морфізм (тобто не відображає всі точки в $\mathcal{O}_{E_2}$), то ϕ є сюр'єктивним відображенням.
- Ядро ізогенії: $\ker(\phi) = \{P \in E_1(\bar{K}) \mid \phi(P) = \mathcal{O}_{E_2}\}$. Ядро завжди є скінченною підгрупою E_1.
- Степінь ізогенії $\deg(\phi)$:
  - Якщо ϕ сепарабельна, $\deg(\phi) = |\ker(\phi)|$.
  - Нульовий морфізм має степінь 0.
- Якщо існує ненульова ізогенія $\phi : E_1 \to E_2$, криві E_1 та E_2 називаються ізогенними.
- Існує дуальна ізогенія $\hat{\phi} : E_2 \to E_1$ така, що $\hat{\phi} \circ \phi = [\deg(\phi)]_{E_1}$ та $\phi \circ \hat{\phi} = [\deg(\phi)]_{E_2}$, де $[m]$ - множення на m. Має той самий степінь: $\deg(\hat{\phi}) = \deg(\phi)$.

Теорема Тейта

Теорема Тейта

Еліптичні криві $E/\mathbb{F}_q$ та $E'/\mathbb{F}_q$ є ізогенними тоді і тільки тоді коли $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$

Ізогенії суперсингулярних кривих

Якщо $E/\mathbb{F}_p$ - суперсингулярна, тоді $j(E)$ визначений в $\mathbb{F}_{p^2}$

Суперсингуляні криві мають ще одну дуже важливу особливість - кільце ендоморфізмів кривої $E/\mathbb{F}_q$: $\mathrm{End}(E)$ ізоморфне деякому ідеалу в алгебрі кватерніонів, тобто поза скалярним добутком $[m] : P \mapsto [m]P$ та ендоморфізмом Фробеніуса $\pi_q : (x, y) \mapsto (x^q, y^q)$ існують ще деякі 2 нетривіальні ендоморфізми(«розмірність алгебри кватерніонів» - 4). Тоді як в ординарному випадку $\pi_q, [m]$ - всі лінійно незалежні ендоморфізми що породжують $\mathrm{End}(E)$

Приклади ізогеній

- Множення на ціле число $[m]$:
  - Для будь-якого цілого $m \neq 0$, відображення $\phi = [m] : E \to E$, що визначається як $P \mapsto P + \cdots + P$ (m разів), є ізогенією (ендоморфізмом).
  - $\ker([m]) = E[m]$ - група точок m-кручення.
  - $\deg([m]) = m^2$.
- Ендоморфізм Фробеніуса π_q (над $\mathbb{F}_q$):
  - Для E над $\mathbb{F}_q$, відображення $\pi_q : (x, y) \mapsto (x^q, y^q)$ є ендоморфізмом.
  - $\ker(\pi_q - [1]) = E(\mathbb{F}_q)$.
  - $\deg(\pi_q) = q$.
  - π_q є чисто несепарабельним.
- Ізогенія факторизації за підгрупою $E \to E/G$:
  - Нехай G - скінченна підгрупа E. Існує (з точністю до ізоморфізму) єдина еліптична крива E' та сепарабельна ізогенія $\phi : E \to E'$ така, що $\ker(\phi) = G$.
  - Криву E' позначають як E/G.
  - $\deg(\phi) = |G|$.

Обчислення ізогеній: Формули Велу (Vélu)

Формули Велу (1971) надають явний алгоритм для обчислення ізогенії $\phi : E \to E/G$ та рівняння кривої E/G, коли задано криву E та її скінченну підгрупу G.

Формули Велу

Нехай $G \subset E(\overline{\mathbb{F}_q})$ - підгрупа E. $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, $(E/G)/\mathbb{F}_q : y^2 = x^3 + a'x + b'$ - еліптичні криві із сепарабельною ізогенією $\phi : E \to E/G$.

$$\phi(Q) = \left(x(Q) + \sum_{P \in G \setminus \{\mathcal{O}\}} (x(Q+P) - x(P)),\ y(Q) + \sum_{P \in G \setminus \{\mathcal{O}\}} (y(Q+P) - y(P))\right)$$

$$a' = a - 5 \sum_{P \in G \setminus \{\mathcal{O}\}} (3x(P)^2 + a), \quad b' = b - 7 \sum_{P \in G \setminus \{\mathcal{O}\}} (5x(P)^3 + 3ax(P) + b)$$

де $x(P)$, $y(P)$ - координати точки P.

Важливо: Формули Велу застосовні для будь-якої скінченної підгрупи G, але обчислення стають складними при зростанні $|G|$, тому зручно обчислювати ізогенії гладких порядків $|G| = l^e$ ітеративно

Граф суперсингулярних l-ізогеній

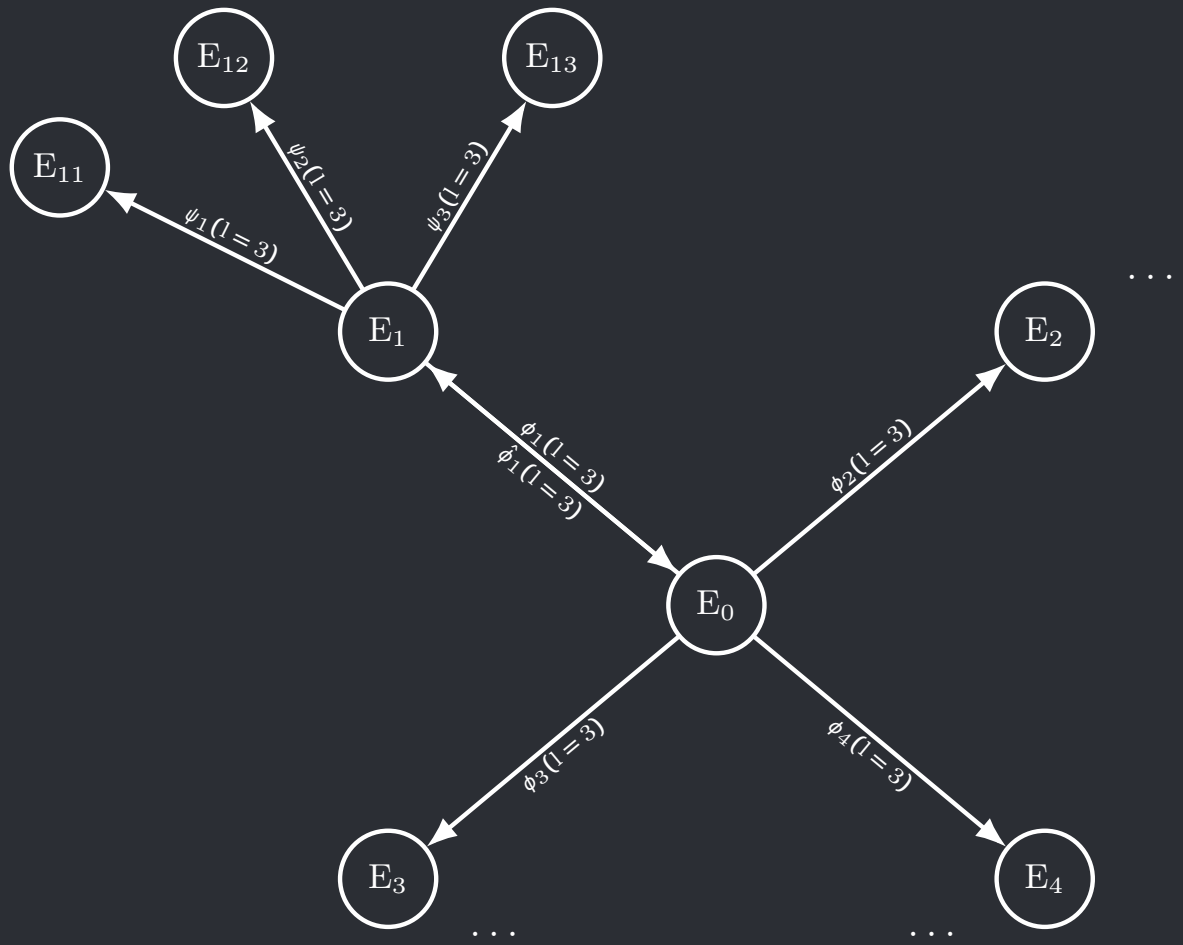
Важливим об'єктом у сучасній криптографії на основі ізогеній є граф суперсингулярних ізогеній.

- Вершини: Множина класів ізоморфізму суперсингулярних еліптичних кривих, визначених над скінченним полем $\mathbb{F}_{p^2}$. Кожен клас ідентифікується своїм j-інваріантом. Кількість таких класів приблизно $p/12$.
- Ребра: Ізогенії малого простого порядку l (наприклад, $l = 2$ або $l = 3$), що з'єднують ці криві. Якщо існує l-ізогенія $\phi : E_1 \to E_2$, то існує і дуальна l-ізогенія $\hat{\phi} : E_2 \to E_1$.

Властивості графу:

- Зв'язність: наслідок теореми Тейта.
- Регулярність: Граф є $(l + 1)$-регулярним $(l \neq p)$
- Експандер (Expander graph): Для більшості параметрів p та l ці графи є експандерами. Це означає, що вони «добре перемішані», і випадкові блукання швидко покривають граф.
- Великий розмір: Кількість вершин значна, що ускладнює повний перебір в задачі пошуку шляху(ізогенії) між двома вершинами (кривими)

Приклад: Локальна структура графу 3-ізогеній



Крива E_0 має 4 різні 3-ізогенії $(\phi_1, \phi_2, \phi_3, \phi_4)$ до кривих E_1, E_2, E_3, E_4. Крива E_1 також має 4 різні 3-ізогенії: одна $(\hat{\phi}_1)$ є дуальною до ϕ_1 і веде назад до E_0, а інші (ψ_1, ψ_2, ψ_3) ведуть до нових кривих E_{11}, E_{12}, E_{13}. Аналогічна структура продовжується для всіх вершин графу.

Складні обчислювальні задачі на основі ізогеній

Припускається, що наступні задачі є обчислювально складними (в тому числі для квантових комп'ютерів):

- Задача знаходження ізогенії (Isogeny Finding Problem): Дано дві ізогенні еліптичні криві E_1, E_2. Знайти явну ізогенію $\phi : E_1 \to E_2$.
- Задача обчислення ендоморфного кільця (Endomorphism Ring Computation): Дано еліптичну криву E. Обчислити її кільце ендоморфізмів $\mathrm{End}(E)$.
- Задача обчислення шляху в графі ізогеній (Supersingular Isogeny Path Problem): Дано дві суперсингулярні еліптичні криві E_0, E_1 та максимальний степінь d. Знайти послідовність ізогеній малих степенів $\phi_1, \ldots, \phi_k$, що сполучає E_0 та E_1, де $\deg(\phi_i) \leq d$.
- Суперсингулярна задача Діффі-Хеллмана (CSIDH/SSIDH Problem): Дано суперсингулярну криву E_0 та образи $E_A = \phi_A(E_0)$, $E_B = \phi_B(E_0)$, де ϕ_A, ϕ_B - невідомі (секретні) ізогенії з певними властивостями. Обчислити j-інваріант спільної кривої $E_{AB} \cong \phi_B(E_A) \cong \phi_A(E_B)$. (Примітка: задача для SIDH виявилася легшою через додаткові точки).

Ці задачі є основою для побудови постквантових криптосистем.

Криптографія на основі ізогеній

- Мотивація: Пошук криптографічних систем, стійких до атак з використанням квантових комп'ютерів (постквантова криптографія, PQC).
- Алгоритм Шора (квантовий) ефективно розв'язує задачі факторизації та дискретного логарифмування (включаючи еліптичні криві), що робить RSA, DH, ECDH вразливими.
- Задачі, пов'язані з ізогеніями (особливо на суперсингулярних кривих), вважаються складними навіть для квантових комп'ютерів (хоча конкретні реалізації, як SIDH, можуть мати вразливості).
- Переваги (потенційні):
  - Стійкість до квантових атак (для певних задач).
  - Відносно малі розміри ключів та шифротекстів порівняно з іншими PQC кандидатами (наприклад, на основі решіток або кодів).
- Недоліки/Виклики:
  - Вища обчислювальна складність порівняно з класичною ECC.
  - Менш досліджена безпека, недавні атаки на основні протоколи (SIDH).

Протокол SIDH: Налаштування (Setup)

Публічні параметри:

- Велике просте число p спеціального вигляду: $p = l_A^{e_A} l_B^{e_B} f \pm 1$, де l_A, l_B - малі різні прості числа, e_A, e_B - великі показники, f - малий кофактор.
- Поле $\mathbb{F}_{p^2}$.
- Стартова суперсингулярна еліптична крива E_0, визначена над $\mathbb{F}_{p^2}$. Структура групи: $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/l_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/l_B^{e_B}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2$
- Базисні точки для підгруп кручення:
  - $\{P_A, Q_A\}$ - базис для $E_0[l_A^{e_A}] = \{P \in E_0(\mathbb{F}_{p^2}) \mid [l_A^{e_A}]P = \mathcal{O}\}$.
  - $\{P_B, Q_B\}$ - базис для $E_0[l_B^{e_B}] = \{P \in E_0(\mathbb{F}_{p^2}) \mid [l_B^{e_B}]P = \mathcal{O}\}$.

  Ці параметри є спільними та відомими всім учасникам.

Протокол SIDH: Ідея обміну ключами

- Мета: Аліса та Боб хочуть встановити спільний секретний ключ.
- Секрети:
- Аліса обирає секретну підгрупу $G_A \subset E_0[l_A^{e_A}]$ порядку $l_A^{e_A}$.
- Боб обирає секретну підгрупу $G_B \subset E_0[l_B^{e_B}]$ порядку $l_B^{e_B}$.
- Ізогенії:
- Аліса обчислює ізогенію $\phi_A : E_0 \to E_A = E_0/G_A$.
- Боб обчислює ізогенію $\phi_B : E_0 \to E_B = E_0/G_B$.
- Обмін: Вони обмінюються інформацією, яка дозволяє кожному обчислити образ секретної підгрупи іншого учасника на своїй кривій.
- Спільний секрет: Обидва обчислюють j-інваріант кривої $E_{AB} \cong E_0/\langle G_A, G_B \rangle$. Завдяки властивостям ізогеній (комутативна діаграма), вони отримають однаковий результат: $j(\phi_B(E_A)) = j(\phi_A(E_B))$.

Далі розглянемо кроки детальніше.

Протокол SIDH: Крок 1 (Секрет та дія Аліси)

1. Вибір секрету: Аліса обирає два випадкових цілих числа $s_A, r_A \pmod{l_A^{e_A}}$ (не обидва нулі, часто $r_A = 1$ і s_A - секрет).
2. Формування ядра: Аліса формує секретну точку (генератор ядра):

$$S_A = P_A + [s_A]Q_A \in E_0[l_A^{e_A}]$$

   Її секретна підгрупа $G_A = \langle S_A \rangle$. Це циклічна підгрупа порядку $l_A^{e_A}$. (Примітка: часто використовують випадкову точку $P_A + [s_A]Q_A$ як генератор)
3. Обчислення ізогенії: Аліса обчислює (за допомогою формул Велу) ізогенію $\phi_A : E_0 \to E_A = E_0/G_A$ гладкого порядку $\deg(\phi_A) = l_A^{e_A}$.
4. Обчислення образів точок Боба: Аліса обчислює образи базисних точок Боба під дією своєї ізогенії: $\phi_A(P_B)$ та $\phi_A(Q_B)$. Ці точки лежать на кривій E_A і мають порядок $l_B^{e_B}$.
5. Надсилання даних: Аліса надсилає Бобу публічний ключ: $(j(E_A), \phi_A(P_B), \phi_A(Q_B))$.

Протокол SIDH: Крок 2 (Секрет та дія Боба)

Аналогічно до Аліси:

1. Вибір секрету: Боб обирає два випадкових цілих числа $s_B, r_B \pmod{l_B^{e_B}}$ (не обидва нулі, часто $r_B = 1$ і s_B - секрет).
2. Формування ядра: Боб формує секретну точку (генератор ядра):

$$S_B = P_B + [s_B]Q_B \in E_0[l_B^{e_B}]$$

   Його секретна підгрупа $G_B = \langle S_B \rangle$ - циклічна порядку $l_B^{e_B}$.
3. Обчислення ізогенії: Боб обчислює ізогенію $\phi_B : E_0 \to E_B = E_0/G_B$ гладкого порядку $\deg(\phi_B) = l_B^{e_B}$.
4. Обчислення образів точок Аліси: Боб обчислює образи базисних точок Аліси:

$$\phi_B(P_A) \quad \text{та} \quad \phi_B(Q_A)$$

   Ці точки лежать на кривій E_B і мають порядок $l_A^{e_A}$.
5. Надсилання даних: Боб надсилає Алісі публічний ключ: $(j(E_B), \phi_B(P_A), \phi_B(Q_A))$.

Протокол SIDH: Крок 3 (Обчислення секрету Алісою)

Аліса отримала $(E_B, \phi_B(P_A), \phi_B(Q_A))$ від Боба.

1. Обчислення образу свого ядра на кривій Боба: Аліса використовує свій секрет s_A (або $S_A = P_A + [s_A]Q_A$) та отримані точки $\phi_B(P_A), \phi_B(Q_A)$, щоб обчислити точку на кривій E_B:

$$S'_A = \phi_B(S_A) = \phi_B(P_A + [s_A]Q_A) = \phi_B(P_A) + [s_A]\phi_B(Q_A)$$

   Ця точка S'_A генерує підгрупу $\phi_B(G_A)$ порядку $l_A^{e_A}$ на кривій E_B.
2. Обчислення фінальної ізогенії: Аліса обчислює ізогенію $\psi_A : E_B \to E_{BA}$, ядром якої є $\langle S'_A \rangle = \phi_B(G_A)$:

$$E_{BA} = E_B/\langle S'_A \rangle = E_B/\phi_B(G_A)$$

3. Спільний секрет: Аліса обчислює j-інваріант кривої E_{BA}.

$$k_A = j(E_{BA})$$

   Це її версія спільного секрету.

Протокол SIDH: Крок 4 (Обчислення секрету Бобом)

Боб отримав $(E_A, \phi_A(P_B), \phi_A(Q_B))$ від Аліси.

1. Обчислення образу свого ядра на кривій Аліси: Боб використовує свій секрет s_B (або $S_B = P_B + [s_B]Q_B$) та отримані точки $\phi_A(P_B), \phi_A(Q_B)$, щоб обчислити точку на кривій E_A:

$$S'_B = \phi_A(S_B) = \phi_A(P_B + [s_B]Q_B) = \phi_A(P_B) + [s_B]\phi_A(Q_B)$$

   Ця точка S'_B генерує підгрупу $\phi_A(G_B)$ порядку $l_B^{e_B}$ на кривій E_A.

2. Обчислення фінальної ізогенії: Боб обчислює ізогенію $\psi_B : E_A \to E_{AB}$, ядром якої є $\langle S'_B \rangle = \phi_A(G_B)$:

$$E_{AB} = E_A/\langle S'_B \rangle = E_A/\phi_A(G_B)$$

3. Спільний секрет: Боб обчислює j-інваріант кривої E_{AB}.

$$k_B = j(E_{AB})$$

   Це його версія спільного секрету.

Протокол SIDH: Комутативність та Спільний Секрет

- Ключова властивість: Ізогенії ϕ_A та ϕ_B мають ядра з порядками, що є взаємно простими ($l_A^{e_A}$ та $l_B^{e_B}$). Це призводить до "комутативності"діаграми (з точністю до ізоморфізму):

$$E_{BA} = E_B/\phi_B(G_A) \cong E_0/\langle G_A, G_B \rangle$$

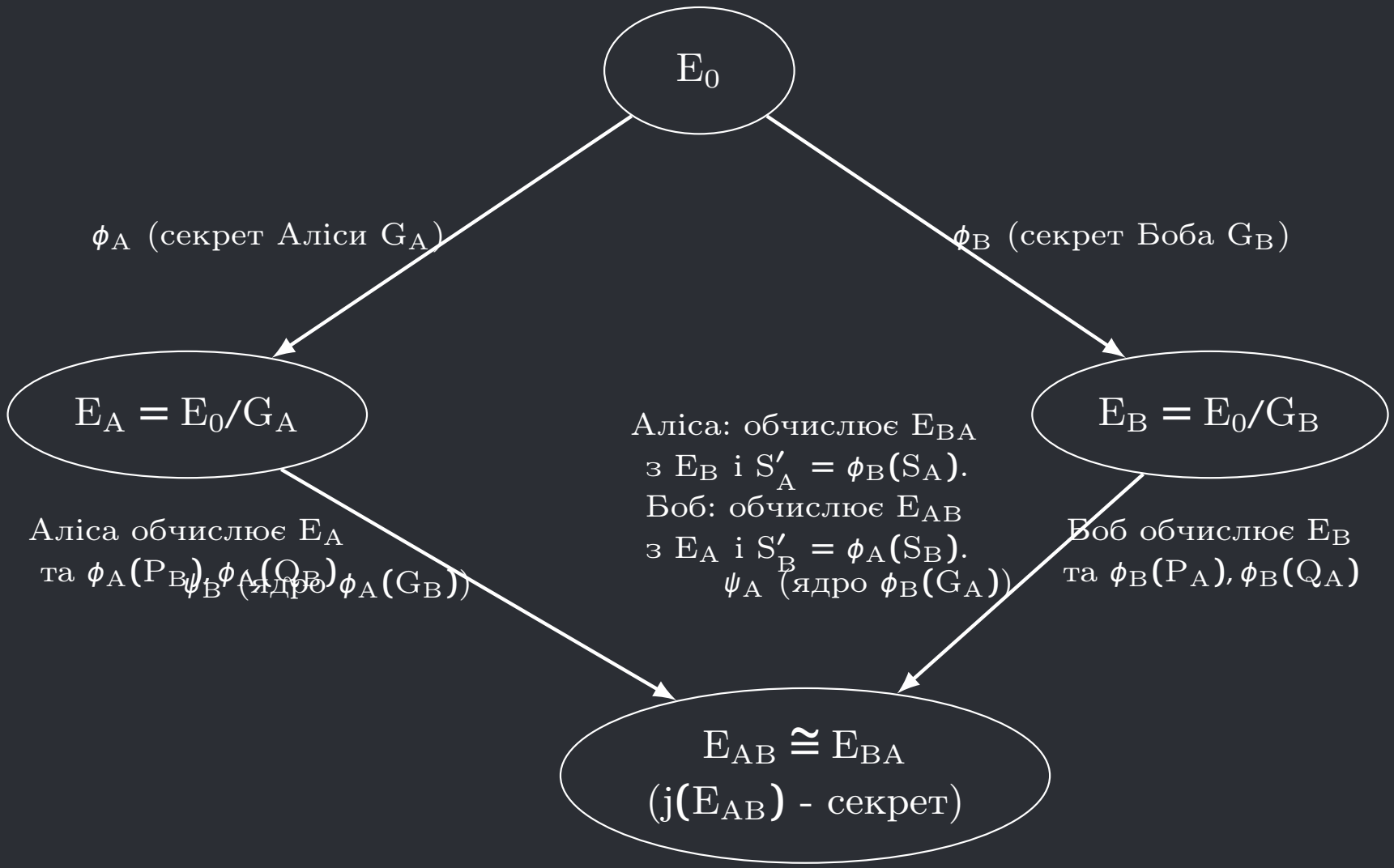
$$E_{AB} = E_A/\phi_A(G_B) \cong E_0/\langle G_A, G_B \rangle$$

  Тому E_{AB}, E_{BA} є ізоморфними над $\mathbb{F}_{p^2}$.
- Спільний секрет: Ізоморфні криві мають однаковий j-інваріант. Отже, Аліса та Боб обчислюють спільний секрет:

$$k_A = j(E_{BA}) = j(E_{AB}) = k_B$$

- Навіщо потрібні $\phi(P), \phi(Q)$? Обчислення $\phi_A(P_B), \phi_A(Q_B)$ (і аналогічно для Боба) є критичним. Воно дозволяє стороні обчислити образ ядра іншої сторони на своїй проміжній кривій (E_A або E_B), не знаючи секретної ізогенії іншої сторони. Саме ці "додаткові точки"(auxiliary points) стали вектором атаки Кастрика-Декру.

Протокол SIDH: Візуалізація



Протокол SIKE (Supersingular Isogeny Key Encapsulation)

- Механізм інкапсуляції ключів (KEM), побудований на основі SIDH.
- Був кандидатом у 3-му та фінальному (4-му) раундах конкурсу постквантової криптографії NIST PQC.
- Використовував перетворення типу Фудзісакі-Окамото для перетворення схеми обміну ключами SIDH (типу PKE) на безпечний KEM (стійкий до атак типу CCA2).
- Основна ідея KEM:
  - KeyGen: Генерує пару ключів (відкритий pk, секретний sk), аналогічно до SIDH.
  - Encaps: Бере відкритий ключ pk отримувача. Генерує випадковий спільний секрет K та його інкапсуляцію (шифротекст) C. Надсилає C отримувачу.
  - Decaps: Отримувач використовує свій секретний ключ sk та отриманий шифротекст C для відновлення того ж спільного секрету K.
- Розглядався як один із найперспективніших кандидатів PQC через малі розміри ключів.
- Став вразливим через атаку на базовий протокол SIDH.

Атака на SIDH/SIKE (Castryck-Decru, 2022)

- У серпні 2022 року Воутер Кастрик (Wouter Castryck) та Тома Декру (Thomas Decru) представили ефективну атаку на протокол SIDH та, як наслідок, на SIKE.
- Ключовий момент: Атака використовує саме ті додаткові точки кручення ($\phi_A(P_B), \phi_A(Q_B)$ та $\phi_B(P_A), \phi_B(Q_A)$), які передаються в протоколі SIDH.
- Ідея атаки (дуже спрощено):
  - Використовує зв'язок між ізогеніями еліптичних кривих та ізогеніями абелевих многовидів вищих розмірностей (зокрема, поверхнями Куммера, пов'язаними з якобіанами гіпереліптичних кривих роду 2).
  - Знання образів додаткових точок дозволяє ефективно відновити інформацію про секретну ізогенію (її ядро, або еквівалентно, секретний скаляр s_A чи s_B).
  - Алгоритм використовує так звані ізогенії Рішело (Richelot isogenies) між якобіанами кривих роду 2, які можна побудувати за допомогою інформації з SIDH.
- Результат: Атака дозволяє відновити секретний ключ Аліси або Боба за поліноміальний час на класичному комп'ютері.
- Це повністю зламало безпеку SIDH та SIKE у їхній відомій формі.

Наслідки атаки та сучасний стан

- SIKE відкликано: NIST відкликав SIKE зі списку кандидатів PQC для стандартизації невдовзі після публікації атаки.
- Пошук нових підходів: Атака стимулювала пошук нових криптографічних схем на основі ізогеній, які б не використовували додаткові точки кручення у такий самий спосіб, або базувалися б на інших варіантах задачі ізогеній (наприклад, CSIDH, яке не використовує $\mathbb{F}_{p^2}$ та додаткові точки).
- Активна область досліджень: Криптографія на основі ізогеній залишається активною, хоча й складнішою, областю досліджень.
- Альтернативні задачі: Розглядаються схеми, що базуються на:
  - Задачі знаходження шляху в графі суперсингулярних ізогеній (без додаткових точок, як у CSIDH).
  - Задачі обчислення ендоморфного кільця.
  - Інших варіантах задачі обчислення ізогеній.

Сучасні алгоритми: SKISign та SQISign

- SKISign (Small Key Isogeny Signature) / SQISign (Short Quaternion Isogeny Signature): Схеми цифрового підпису на основі ізогеній. SQISign є новішою та ефективнішою версією.
- Інша базова задача: Безпека базується на складності задачі знаходження ізогенійного шляху між двома заданими суперсингулярними кривими (Supersingular Isogeny Path Problem) та пов'язаних задачах у графі ізогеній. SQISign також використовує структуру кватерніонних алгебр.
- Не використовує SIDH-структуру: Схеми побудовані інакше і не використовують обмін додатковими точками, як у SIDH. Тому атака Кастрика-Декру на них безпосередньо не застосовується.
- Ідея підпису (GPS/Fiat-Shamir): Схема використовує підхід типу доказу з нульовим розголошенням (перетворений на підпис за допомогою Fiat-Shamir), де доказом знання секрету (секретного шляху ізогеній) є здатність відповісти на криптографічний виклик.
- Переваги: Постквантова стійкість, дуже малі розміри підписів (особливо SQISign) порівняно з іншими PQC підписами.
- Недоліки: Досить повільна генерація та перевірка підпису.

Висновки

- Ізогенії є фундаментальними об'єктами в теорії еліптичних кривих, що описують структурні зв'язки між ними.
- Формули Велу дозволяють явно обчислювати ізогенії за їхніми ядрами.
- Складність обчислення ізогеній (особливо між суперсингулярними кривими) стала основою для розробки постквантових криптосистем.
- Протоколи SIDH/SIKE були перспективними, але виявилися вразливими через використання додаткової інформації (точок кручення).
- Атака 2022 року стала важливим уроком для спільноти PQC.
- Дослідження продовжуються, фокусуючись на альтернативних задачах та конструкціях (CSIDH, SQISign), що демонструє життєздатність напрямку, хоч і з новими викликами.