Curves With Complex Multiplication & Applications To Cryptography

Bianca Viray, University of Washington

SIAM Conference on Applied Algebraic Geometry
Georgia Institute of Technology
August 2, 2017
Diffie-Hellman Key Exchange

Fix a group $G$ and an element $g \in G$.

**Alice**
- Chooses secret $a \in \mathbb{Z}$
- Computes $A = g^a$
- Computes $B^a$

**Bob**
- Chooses secret $b \in \mathbb{Z}$
- Computes $B = g^b$
- Computes $A^b$

**Shared secret**
\[(g^b)^a = g^{ab} = (g^a)^b\]
Implementation

Need a cyclic group \( G = \langle g \rangle \) such that

- Exponentiation or multiplication is fast, &
- Given \( h \in \langle g \rangle \), it is hard to find \( x \in \mathbb{Z} \) s.t. \( h = g^x \)

**Discrete logarithm problem (DLP)**

Alice \[ A = g^a \] \[ B = g^b \] \[ (g^b)^a = g^{ab} = (g^a)^b \] Bob
Implementation

Need a cyclic group $G = \langle g \rangle$ such that

- Exponentiation or multiplication is fast, &
- Given $h \in \langle g \rangle$, it is hard to find $x \in \mathbb{Z}$ s.t. $h = g^x$

DLP for $G$ is only as hard as the DLP for $G_p$, the cyclic subgroup of largest prime order.
Examples

\[ G = (\{0, 1, \ldots, p-1\}, + \mod p), g \in G \text{ generator} \]

DLP: Given \( a \in G \), find \( x \in \mathbb{Z} \) s.t. \( a = xg \mod p \)

\[ \iff \text{find } x, y \in \mathbb{Z} \text{ s.t. } a = xg + yp \]

BAD!

Extended euclidean algorithm solves in \( O(\log p) \) time
Sanity Check

Isn’t every cyclic group of order $p$ isomorphic to $(\{0, 1, \ldots, p-1\}, + \text{ mod } p)$?

Let $G$ be a cyclic group of order $p$ and let $g$ a generator.

There exists a unique homomorphism

$$\varphi: G \rightarrow (\{0, 1, \ldots, p-1\}, + \text{ mod } p), \varphi(g) = 1$$

For $a \in G$, determining $\varphi(a)$ is equivalent to solving DLP for $a$.!
More Examples

- $G \leq \mathbb{F}_q^\times$ Not as bad as $\mathbb{Z}$ mod $p$, but not optimal. Need to take $|G| \sim 2^{3072}$

- Matrix groups Too much structure

- Groups from algebraic geometry?
Let $k$ be a field and let $C$ be a nice curve over $k$.

E.g., $C: \quad y^2z = x^3 + xz^2 + 2z^3 \quad \subset \mathbb{P}^2$

$C: \quad y^2 = x^6 + z^6 \quad \subset \mathbb{P}(1,3,1)$

Given a nice curve $C$, we obtain an abelian group

$\text{Jac}(C) = \text{Div}^0(C)/\text{Princ}(C)$
Genus 1

C genus 1 with a point, then \( \text{Jac}(C) \cong C \).
Genus 2

C genus 2, then $\text{Jac}(C) \cong \text{Sym}^2(C)$. 
Genus 2

C genus 2, then $\text{Jac}(C) \cong \text{Sym}^2(C)$. 
Are Jacobians Suitable For Cryptography?

Need a large prime order group $G = \langle g \rangle$ s.t.

1. Exponentiation or multiplication is fast, &
2. Given $h \in G$, it is hard to find $x \in \mathbb{Z}$ s.t. $h = g^x$

- $C$ genus $g$ over $\mathbb{F}_q$, then $\#Jac(C) \sim q^g$
- Multiplication efficient in low genus (lots of work!)
- No known efficient attacks in low genus
How do we obtain a curve $C/F_q$ such that $\#\text{Jac}(C)$ is prime?

1. **Search!** Randomly generate curves and check whether $\#\text{Jac}(C)$ is prime.
   Works well for $g=1$, just becoming feasible for $g=2$

2. **Construct?** Use the CM method
   (Atkin-Morain, Spallek, van Wamelen, Weng)
Order Of Jacobian

For any curve $C/F_\mathbb{Q}$, there is a Frobenius endomorphism $\pi \in \text{End}^0(\text{Jac}(C))$.

$\#\text{Jac}(C)$ is determined by $\min_{\pi}(x)$ and $\min_{\pi}(x)$ essentially determined by $\mathbb{Q}(\pi) \subset \text{End}^0(\text{Jac}(C))$.

In many cases, $\mathbb{Q}(\pi) = \text{End}^0(\text{Jac}(C))$. 
Order Of Jacobian

If we can determine $Q(\pi)$, then we can compute $\#\text{Jac}(C)$.

So how does this help?

If $[Q(\pi):Q] = 2g(C)$, then $Q(\pi)$ is a CM field, a totally imaginary quad. extension of a totally real field.

For a fixed CM field $K$ of degree $2g$, genus $g$ complex curves with CM by $K$ are completely understood!
Complex Multiplication

Let $K$ be a primitive CM field of degree $2g$.

- There are finitely many complex isomorphism classes of genus $g$ curves with CM by $K$.
- Complex approximations of the isomorphism invariants of such curves can be computed to arbitrary precision.
- Each genus $g$ curve with CM by $K$ is defined over a number field, and for each there are infinitely many primes such that the reduction has CM by $K$. 
Complex Multiplication

Genus 1 case: fix $K$ imaginary quadratic field

\[ H_K(x) := \prod (x - j(C)) \in \mathbb{Z}[x] \]

$C$ with CM by $K$

Can recognize coefficients from complex approximations

Genus 2 case: fix $K$ primitive quartic CM field

For $n=1,2,3, H_{K,n}(x) := \prod (x - i_n(C)) \in \mathbb{Q}[x]$

$C$ with CM by $K$

Need a bound on denominators to recognize the coefficients!
Let $p$ be a prime appearing in the denominator of a coefficient of $H_{K,n}(x) := \prod (x - i_n(C))$. Then there is some curve $C$ with CM by $K$ and some prime $\mathfrak{p} | p$ such that $i_n(C) \equiv \infty \mod \mathfrak{p}$. 
Let $p$ be a prime appearing in the denominator of a coefficient of $H_{K,n}(x) := \prod (x - i_n(C))$.

Then there is some curve $C$ with CM by $K$ and some prime $\mathfrak{p}|p$ such that $i_n(C \mod \mathfrak{p}) = \infty$.

So $C$ has bad reduction at $\mathfrak{p}$!
Interpreting Denominators Moduli-Theoretically

Let $p$ be a prime appearing in the denominator of a coefficient of $H_{K,n}(x) := \prod (x - i_n(C))$.

Then there is some curve $C$ with CM by $K$ and some prime $p | p$ such that $i_n(\text{Jac}(C) \mod p) = \infty$.

So $\text{Jac}(C) \mod p \ldots$
Interpreting Denominators Moduli-Theoretically

Let $p$ be a prime appearing in the denominator of a coefficient of $H_{K, n}(x) := \prod (x - i_n(C))$.

Then there is some curve $C$ with CM by $K$ and some prime $p | p$ such that $i_n(\text{Jac}(C) \mod p) = \infty$.

So $\text{Jac}(C) \mod p$ is isomorphic to a product $E \times E'$. 
If a prime $p$ appears in the denominator of a coefficient of $H_{K,n}(x) := \prod (x - i_n(C))$

$\mathbb{C}$ with CM by $K$

Then there are elliptic curves $E, E' / \overline{\mathbb{F}_p}$ such that $O_K \subset \text{End}(ExE')$. 
Interpreting Denominators Moduli-Theoretically

With more care, this argument can give more precise information.

For fixed $K$ and $p$, we have

$$v_p(\text{denoms}) \sim \# \{ E, E' / F_p : \mathcal{O}_K \subseteq \text{End}(ExE') \}$$

(counted with multiplicity and up to automorphism)
Recap

- For secure genus 2 DH key exchange, need a genus 2 curve $\mathbb{C}/\mathbb{F}_q$ s.t. $\#\text{Jac}(\mathbb{C}) = \text{large prime}$.

- To construct such a $\mathbb{C}/\mathbb{F}_q$, use the CM method.

- To determine the precision needed for CM method, bound the denominators of $H_{K,n}(x)$.

- To bound, need to understand $(\text{CM}(K).\text{Prod})_p \sim \#\{ E, E' / \mathbb{F}_p : \mathcal{O}_K \subset \text{End}(E \times E') \}$
Theorem (Yang, Conj. by Bruinier-Yang)

If $K$ has very mild ramification, then there exists an explicit formula for $(CM(K).\text{Prod})_p$ for all primes $p$.

Following Kudla’s program, also related $(CM(K).\text{Prod})$ to coefficients of Eisenstein series. This relation was proved in general by Howard-Yang, but no explicit formula was given.
Theorem (Lauter, Viray)

For all $K$, there exists an algorithm for computing $(CM(K).Prod)$. If $K$ is "nice enough" then there exists an explicit formula.

Bouyer and Streng: Computed all CM genus 2 curves defined over the real quadratic subfield of the reflex field. Using LV formula, showed their computations were provably correct.
Proof follows “embedding problem” approach laid out by Goren and Lauter: count the number of elliptic curves $E$, $E'$ and embeddings

$$O_K \rightarrow \begin{pmatrix} \text{End}(E) & \text{Hom}(E',E) \\ \text{Hom}(E,E') & \text{End}(E') \end{pmatrix}$$

Since $K$ is a primitive quartic CM field, the existence of such an embedding implies that $E$ and $E'$ are supersingular.
Tools

Get an upper bound from the arithmetic intersection number

\[ \text{CM}(O_d) \cdot \text{CM}(O_{d'}) \]

on moduli space of elliptic curves.

Gross and Zagier formula if \( O_d \) and \( O_{d'} \) maximal & \( \gcd(d, d') = 1 \); LV formula/algorithms in general
Tools

To go from the aforementioned upper bound to an exact formula, need to understand when an endomorphism of $E$ can be factored as 2 isogenies with certain properties.
Recap

• Use embedding problem and \((\text{CM}(O_d).\text{CM}(O_{d'}))\) to bound denominators of \(H_{K,n}(x)\) [LV].

• Use this bound to determine precision needed for CM method.

• Use CM method + [Mestre] to construct a \(C/F_q\) s.t. \#Jac(C) = large prime.

• Use curve to implement DH key exchange system (or El Gamal PKC).
Thank you!