Constructing Abelian Varieties for Pairing-Based Cryptography

David Mandell Freeman

CWI and Universiteit Leiden, Netherlands

Workshop on Pairings in Arithmetic Geometry and Cryptography

4 May 2009
What is pairing-based cryptography?

- “Pairing-based cryptography” refers to protocols that use a nondegenerate, bilinear map

\[ e : G_1 \times G_2 \rightarrow G_T \]

between finite, cyclic groups.
- Group operations and pairing need to be easily computable.
- Need *discrete logarithm problem* (DLP) in \( G_1, G_2, G_T \) to be infeasible.
- DLP: Given \( x, x^a \), compute \( a \).
Example: Boneh-Lynn-Shacham signatures

- Setup:
  - Bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
  - Public $P, Q \in \mathbb{G}_1$.
  - Secret $a \in \mathbb{Z}$ such that $Q = Pa$.
  - Hash function $H : \{0, 1\}^* \to \mathbb{G}_2$.

- Signature on message $m$ is $\sigma = H(m)^a$.

- To verify signature: see if $e(Q, H(m)) = e(P, \sigma)$.
  - If signature is correct, then both equal $e(P, H(m))^a$.
  - If DLP is infeasible, then signature cannot be forged.
Useful pairings: Abelian varieties over finite fields

- For certain abelian varieties $A/\mathbb{F}_q$, subgroups of $A(\mathbb{F}_q)$ of prime order $r$ have the desired properties.
- Pairings are *Weil pairing*
  \[ e_r : A[r] \times A[r] \rightarrow \mu_r \subset \mathbb{F}_{q^k}^\times \]
  or *Tate pairing*
  \[ \tau_r : A(\mathbb{F}_{q^k})[r] \times A(\mathbb{F}_{q^k})/rA(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r \cong \mu_r(\mathbb{F}_{q^k}) \]
- $k$ is the *embedding degree* of $A$ with respect to $r$.
  - Smallest integer such that $\mu_r \subset \mathbb{F}_{q^k}^\times$
- If $q, r$ are large, DLP is infeasible in $A[r]$ and $\mathbb{F}_{q^k}^\times$.
- If $A = \text{Pic}^0(C)$, pairings can be computed efficiently via Miller’s algorithm.
Need to “balance” security on variety and in finite field

- Best DLP algorithm in $A[r]$ is exponential-time.
- Best DLP algorithm in $\mathbb{F}_q^\times$ is subexponential-time.
- For comparable security before and after pairing, need $q^k > r$.
- How much larger depends on desired security level:

<table>
<thead>
<tr>
<th>$r$ (bits)</th>
<th>$q^k$ (bits)</th>
<th>Embedding degree $k$ (if $r \approx q^g$)</th>
<th>Secure until year</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>1024</td>
<td>$6g$</td>
<td>2010</td>
</tr>
<tr>
<td>224</td>
<td>2048</td>
<td>$10g$</td>
<td>2030</td>
</tr>
<tr>
<td>256</td>
<td>3072</td>
<td>$12g$</td>
<td>2050</td>
</tr>
</tbody>
</table>
The Problem

Find primes $q$ and abelian varieties $A/\mathbb{F}_q$ having

1. a subgroup of large prime order $r$, and
2. prescribed (small) embedding degree $k$ with respect to $r$.

- In practice, want $r > 2^{160}$ and $k \leq 50$.

We call such varieties *pairing-friendly*.

Want to be able to control the number of bits of $r$ to construct varieties at varying security levels.
“Random” abelian varieties not useful for pairing-based cryptography

- Embedding degree $k$ is the order of $q$ in $(\mathbb{Z}/r\mathbb{Z})^*$.
- Embedding degree of random $A/\mathbb{F}_q$ with order-$r$ subgroup will be $\approx r$.
  - Precise formulation for elliptic curves by Bal.-Koblitz.
- Typical $r > 2^{160}$, so pairing on random $A$ can’t even be computed.
- Conclusion: pairing-friendly abelian varieties are “special.”
Outline

Pairing-Friendly Abelian Varieties
   Pairings and Cryptography
   Ordinary vs. Supersingular
   Frobenius and complex multiplication

MNT Type Methods
   The MNT Method
   Extending the MNT Method

Cocks-Pinch Type Methods
   The Cocks-Pinch Method
   The Brezing-Weng Method
   Extending to Higher Dimensions

Summary
Supersingular abelian varieties are always pairing-friendly

- An elliptic curve $E/\mathbb{F}_q$ is supersingular if $\#E[p] = 1$.
- A $g$-dimensional abelian variety $A/\mathbb{F}_q$ is supersingular if $A$ is isogenous (over $\overline{\mathbb{F}}_q$) to a product of $g$ supersingular elliptic curves.
- Supersingular AV are easy to construct.
- Menezes-Okamoto-Vanstone: supersingular elliptic curves have embedding degree $k \in \{1, 2, 3, 4, 6\}$.
  - $k = 4, 6$ only possible in char 2, 3, respectively.
- Galbraith: If $A/\mathbb{F}_q$ is supersingular, then $k$ is bounded by constant $k_0(g)$.
- Rubin-Silverberg: If $g \leq 6$ then $k_0(g) \leq 7.5g$. 

Ordinary abelian varieties

- If we want $k > 7.5g$ we must use non-supersingular (usually, *ordinary*) abelian varieties.
- An abelian variety $A/\mathbb{F}_q$ is *ordinary* if $\#A[p] = p^g$.
- Assume from now on that $A$ is ordinary and simple.
  - Ignore intermediate cases $\#A[p] = p^e$, $0 < e < g$. 
Complex multiplication: the basics

- For ordinary, simple, \(g\)-dimensional \(A/\mathbb{F}_q\), \(\text{End}(A) \otimes \mathbb{Q}\) is a \textit{CM field} \(K\) of degree \(2g\).
  - \(K\) is an imaginary quadratic extension of totally real field.
- \textit{Frobenius endomorphism} \(\pi : (x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)\) satisfies \(f(\pi) = 0\) for \(f \in \mathbb{Z}[x]\) monic of degree \(2g\).
- Honda-Tate theory: \(K = \text{End}(A) \otimes \mathbb{Q} \cong \mathbb{Q}[x]/(f(x))\).
- Furthermore, \(\pi\) is a \textit{q-Weil number} in \(\mathcal{O}_K\).
  - All embeddings \(K \hookrightarrow \mathbb{C}\) have \(\pi \bar{\pi} = q\).
Properties of Frobenius make $A / \mathbb{F}_q$ pairing-friendly

- Number of points given by $\# A(\mathbb{F}_q) = f(1) = N_{K / \mathbb{Q}}(\pi - 1)$.
- Embedding degree $k$ is order of $q = \pi \overline{\pi}$ in $(\mathbb{Z}/r\mathbb{Z})^\times$.
- $A$ has embedding degree $k$ with respect to prime $r \nmid kq$ iff
  1. $A(\mathbb{F}_q)$ has a subgroup of order $r$
     $\iff N_{K / \mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}$
  2. $q$ has order $k$ in $(\mathbb{Z}/r\mathbb{Z})^*$
     $\iff \Phi_k(q) = \Phi_k(\pi \overline{\pi}) \equiv 0 \pmod{r}$
     ($\Phi_k = k$th cyclotomic polynomial).
- Construction procedure:
  1. Fix $K$, construct $\pi \in \mathcal{O}_K$ with properties (1) and (2).
  2. Use Complex Multiplication methods to produce an explicit abelian variety over $\mathbb{F}_q$ with Frobenius endomorphism $\pi$ ($q = \pi \overline{\pi}$).
The Complex Multiplication Method
(Atkin, Morain)

- Given a Frobenius element $\pi$ in a CM field $K$:
  1. List the abelian varieties in characteristic zero with CM by $\mathcal{O}_K$.
  2. Reduce modulo primes over $q = \pi \overline{\pi}$.
  3. Some twist of one of the reduced varieties has Frobenius endomorphism $\pi$. Use (probabilistic) point counting to find it.

- Method is exponential in the discriminant of $K$ and is only well-developed for dimension 1 and 2.

- In practice: choose $K$ for which CM method is known to be feasible, and construct $\pi \in K$. 
Outline

Pairing-Friendly Abelian Varieties
  Pairings and Cryptography
  Ordinary vs. Supersingular
  Frobenius and complex multiplication

MNT Type Methods
  The MNT Method
  Extending the MNT Method

Cocks-Pinch Type Methods
  The Cocks-Pinch Method
  The Brezing-Weng Method
  Extending to Higher Dimensions

Summary
Some Properties of Ordinary Elliptic Curves

- \( \pi \) satisfies \( x^2 - tx + q = 0 \), where \( t = \pi + \overline{\pi} \).
- Can write \( \pi = \frac{1}{2}(-t \pm \sqrt{t^2 - 4q}) \).
- Hasse: \( t^2 - 4q = -Dy^2 \) for \( D > 0 \) square-free. This is the \textit{CM equation}.
- CM field \( K \) is \( \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q}) = \mathbb{Q}(\sqrt{-D}) \).
  - Choosing a quadratic CM field \( K \) is equivalent to choosing a square-free \( D > 0 \).
- \( \#E(\mathbb{F}_q) = q + 1 - t \). Consequences:
  1. Embedding degree condition \( r \mid \Phi_k(q) \) can be replaced with \( r \mid \Phi_k(t - 1) \).
    - \( r \) divides \( q + 1 - t \) implies \( q \equiv t - 1 \) (mod \( r \)).
  2. Can rewrite CM equation as \( Dy^2 = 4hr - (t - 2)^2 \)
    - \( h \) is a “cofactor” satisfying \( \#E(\mathbb{F}_q) = hr \).
    - Set \( h = 1 \) if we want \( \#E(\mathbb{F}_q) \) to be prime.
    (Assume \( h = 1 \) from now on.)
Overview of the Miyaji-Nakabayashi-Takano Method

- For fixed $D, k$, we are looking for $t, r, q, y$ satisfying certain divisibility conditions and the CM equation

$$Dy^2 = 4r - (t - 2)^2.$$  

- Idea: Parametrize $t, r, q$ as polynomials $t(x), r(x), q(x)$.
- MNT method: Choose $t(x)$, compute $r(x)$ satisfying divisibility conditions, solve CM equation in 2 variables $x, y$.  

The MNT Method

For fixed $D, k$, find $t, r, q, y$ with

\[
\begin{align*}
  r &= q + 1 - t \\
  r &| \Phi_k(t - 1) \\
  Dy^2 &= 4r - (t - 2)^2
\end{align*}
\]

1. Fix $k$ and (small) $D$, and choose polynomial $t(x)$.
2. Choose $r(x)$ an irreducible factor of $\Phi_k(t(x) - 1)$.
3. Compute $q(x) = r(x) + t(x) - 1$.
4. Find integer solutions $(x_0, y_0)$ to CM equation (3).
5. If $q(x_0), r(x_0)$ are both prime for some $x_0$, use CM method to construct elliptic curve with Frobenius $\pi = \frac{1}{2}(-t(x_0) + y_0 \sqrt{-D})$. 
Obstacles to the MNT Method

- Step 4 is the difficult part: finding integer solutions $(x_0, y_0)$ to

\[ Dy^2 = 4r(x) - (t(x) - 2)^2. \]

- If $f(x) = 4r(x) - (t(x) - 2)^2$ has degree $\geq 3$ and no multiple roots, then $Dy^2 = f(x)$ has only a finite number of integer solutions! (Siegel’s theorem)

- Consequence: need to choose $t(x), r(x)$ so that $f(x)$ is quadratic or has multiple roots.

- This is hard to do for $k > 6$, since $\deg r(x)$ must be a multiple of $\varphi(k) > 2$. 
The MNT Solution for $k = 3, 4, 6$

Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_k(t(x) - 1)$, such that $f(x) = 4r(x) - (t(x) - 2)^2$ is quadratic.

Solution when $\varphi(k) = 2$:
1. Choose $t(x)$ linear $\Rightarrow$ $r(x)$ is quadratic $\Rightarrow$ so is $f(x)$.
2. Use standard algorithms to find solutions $(x_0, y_0)$ to $Dy^2 = f(x)$.
3. If no solutions of appropriate size, or $q(x)$ or $r(x)$ not prime, choose different $D$ and try again.

Construction depends on finding integer solutions to a “Pell-like equation” $z^2 - D'y^2 = C$.

Solutions grow exponentially $\Rightarrow$ MNT curves of prime order are sparse (Luca-Shparlinski).
Extending the MNT method

- Galbraith-McKee-Valença: extend MNT idea by allowing cofactor $h \neq 1$, so that $\#E(\mathbb{F}_p) = h \cdot r(x)$.
  - Find many more suitable curves than original MNT construction.
  - $h = 4$ allows curves to be put in Edwards form (see Vercauteren, Naehrig talks).
F. Solution for $k = 10$

- Goal: Choose $t(x)$, find factor $r(x)$ of $\Phi_{10}(t(x) - 1)$, such that $f(x) = 4r(x) - (t(x) - 2)^2$ is quadratic.
  - All factors of $\Phi_{10}(t(x) - 1)$ must have $4 \mid \text{degree}$.
- Key observation: Need to choose $r(x), t(x)$ such that the leading terms of $4r$ and $t^2$ cancel out.
  - Smallest possible case: $\deg r = 4, \deg t = 2$.
- Galbraith-McKee-Valença: Characterized quadratic $t(x)$ such that $\Phi_{10}(t(x) - 1)$ factors into two quartics.
- One of these $t(x)$ gives the desired cancellation!
- Construct curves via Pell-like equation as in MNT solution.
  - Like MNT curves, $k = 10$ curves are sparse.
  - Can’t be extended to allow cofactors $h \neq 1$. 
MNT Method in Higher Dimensions?

- MNT method depends essentially on finding integral points on the variety defined by the CM equation $Dy^2 = f(x)$.
- CM equation relates CM field $K = \mathbb{Q}(\pi)$ to number of points on pairing-friendly variety.
- In elliptic curve case, CM equation defines a plane curve
  - Lots of points if genus 0; otherwise not enough.
- Analogous equations in dimension 2 (F. ‘07) define a much more complicated variety.
  - No idea how to find integral points.
- Nothing known in dimension $\geq 3$.
- Conclusion: in dimension $\geq 2$ we have no idea how to construct pairing-friendly ordinary abelian varieties with a prime number of points!
Outline

Pairing-Friendly Abelian Varieties
  Pairings and Cryptography
  Ordinary vs. Supersingular
  Frobenius and complex multiplication

MNT Type Methods
  The MNT Method
  Extending the MNT Method

Cocks-Pinch Type Methods
  The Cocks-Pinch Method
  The Brezing-Weng Method
  Extending to Higher Dimensions

Summary
Overview of the Cocks-Pinch Method

- Recall: for an elliptic curve with embedding degree $k$ and Frobenius element $\pi \in K = \mathbb{Q}(\sqrt{-D})$ we want

\[
N_{K/Q}(\pi - 1) \equiv 0 \pmod{r} \quad (1)
\]
\[
\Phi_k(\pi \pi^{-1}) \equiv 0 \pmod{r} \quad (2)
\]

for some prime subgroup order $r$.

- Suppose $r$ factors as $\tau \overline{\tau}$ in $\mathcal{O}_K$, and

\[
\pi \equiv 1 \pmod{\tau}
\]
\[
\pi \equiv \zeta_k \pmod{\overline{\tau}}
\]

\[
(\iff \overline{\pi} \equiv \zeta_k \pmod{\tau})
\]

for a primitive $k$th root of unity $\zeta_k \in \mathbb{F}_r$.

- Then (1) and (2) are satisfied!
The Cocks-Pinch Construction

1. Choose CM field $K = \mathbb{Q}(\sqrt{-D})$, embedding degree $k$, and prime $r \equiv 1 \pmod{k}$ with $r = t\bar{t}$ in $\mathcal{O}_K$.
2. Use Chinese Remainder thm to construct $\pi \in \mathcal{O}_K$ with
   \[
   \begin{align*}
   \pi &\equiv 1 \pmod{t} \\
   \pi &\equiv \zeta_k \pmod{\bar{t}}
   \end{align*}
   \]
3. Add elements of $r\mathcal{O}_K$ until $q = \pi\bar{\pi}$ is prime.
4. The resulting $\pi$ is the Frobenius of an elliptic curve $E/\mathbb{F}_q$ that has embedding degree $k$ with respect to a subgroup of order $r$.
5. Use CM method to determine equation for $E$. 

Analyzing the Cocks-Pinch Construction

- $\pi$ is “randomish” element of $\mathcal{O}_K/r\mathcal{O}_K$  
  $\Rightarrow \pi$ should have norm $q = \pi\overline{\pi} \approx r^2$.

- $q$ is “randomish” integer $\approx r^2$, so we expect to try $\approx 2\log r$ different lifts $\pi$ to find one with prime norm.

- How efficient are Cocks-Pinch curves?
  - Define $\rho = \frac{\log q}{\log r} = \frac{\# \text{bits of } q}{\# \text{bits of } r}$.
  - If keys, signatures, ciphertexts, etc. are elements of $E[r]$, we want $\rho$ small to save bandwidth.
  - If curve has prime order, $\rho = 1$.
  - Cocks-Pinch curves have $\rho \approx 2$.

- Can we do better?
The Brezing-Weng Idea

- Cocks-Pinch construction: CM field $K = \mathbb{Q}(\sqrt{-D})$, embedding degree $k$, prime $r$, with
  1. $r = \tau \bar{\tau}$ in $\mathcal{O}_K$,
  2. $\mu_k \subset (\mathbb{Z}/r\mathbb{Z})^*$.

- Brezing-Weng idea: choose $r$ to be an irreducible polynomial $r(x) \in \mathbb{Q}[x]$ with
  1. $r(x) = \tau(x)\bar{\tau}(x)$ in $K[x]$,
  2. $\mu_k \subset \mathbb{Q}[x]/(r(x))$.

- Use Chinese Remainder theorem in $K[x]$ to construct $\pi(x) \in K[x]$ with
  $$\pi(x) \equiv 1 \mod \tau(x)$$
  $$\pi(x) \equiv \zeta_k \mod \bar{\tau}(x)$$

- Evaluate $\pi(x)$ at $x_0$ to get Frobenius element $\pi \in \mathcal{O}_K$. 
Analyzing the Brezing-Weng Method

- Method produces $\pi(x) \in K[x]$ such that for many $x_0 \in \mathbb{Z}$, $\pi(x_0) \in \mathcal{O}_K$ satisfies the pairing-friendly conditions.

- Choose integers $x_0$ until $q(x_0) = \pi(x_0)\overline{\pi}(x_0)$ is prime and $r(x_0)$ is (nearly) prime.

- Use CM method to construct $E/\mathbb{F}_{q(x_0)}$ with Frobenius $\pi(x_0)$.

- Key observation: $\deg \pi(x) < \deg r(x)$, therefore $q(x_0) < r(x_0)^2$.
  - Can always obtain $\rho < 2$, improving on Cocks-Pinch method.
How to choose Brezing-Weng Parameters?

- Choices: CM field $K = \mathbb{Q}(\sqrt{-D})$, embedding degree $k$, polynomial $r(x)$
  - Need $\mathbb{Q}(\sqrt{-D}, \zeta_k) \subset L = \mathbb{Q}[x]/(r(x))$.
- Best success when $L$ is a cyclotomic field, $D$ small.

Examples:

1. Brezing-Weng: $D = 1, 2, 3$, $r(x) = \Phi_k(x)$.
   - Achieve e.g., $\rho = 5/4$ for $k = 24$ with $D = 3$
2. Barreto-Naehrig: Cleverly choose $u(x)$ such that $\Phi_k(u(x))$ factors into $r(x)r(-x)$.
   - Achieve $\rho = 1$ (prime order!) for $k = 12$ with $D = 3$.
3. Kachisa-Schaefer-Scott: Brute-force search in space of polynomials defining $\mathbb{Q}(\zeta_k)$.
   - Achieve e.g., $\rho = 9/8$ for $k = 32$ with $D = 1$.

- See F.-Scott-Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves."
Generalizing the Cocks-Pinch Method (F.-Stevenhagen-Streng)

- Want to construct $g$-dimensional pairing-friendly ordinary abelian varieties.
- Easiest case: CM field $K$ Galois cyclic, degree $2g$, $\text{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$.
- Subgroup order $r$ is a prime that splits completely in $K$.
- Pick a prime $\mathfrak{r}$ over $r$ in $\mathcal{O}_K$, and write

$$r\mathcal{O}_K = \mathfrak{r} \cdot \mathfrak{r}^\sigma \cdots \mathfrak{r}^{\sigma^{g-1}} \cdot \overline{\mathfrak{r}} \cdot \overline{\mathfrak{r}}^\sigma \cdots \overline{\mathfrak{r}}^{\sigma^{g-1}}$$

(note $\sigma^g = \text{complex conjugation}$).
Constructing a π with prescribed residues

\[ r \mathcal{O}_K = r \cdot r^\sigma \cdots r^{\sigma^{g-1}} \cdot \bar{r} \cdot \bar{r}^\sigma \cdots \bar{r}^{\sigma^{g-1}} \]

Given \( \xi \in \mathcal{O}_K \), write residues of \( \xi \) modulo primes over \( r \) as

\[ (\alpha_1, \alpha_2, \ldots, \alpha_g, \beta_1, \ldots, \beta_g) \in \mathbb{F}_r^{2g}. \]

Then residues of \( \xi^{\sigma^{-1}} \) are

\[ (\alpha_2, \alpha_3, \ldots, \beta_1, \beta_2, \ldots, \alpha_1) \in \mathbb{F}_r^{2g}, \]

and so on for each \( \xi^{\sigma^{-i}} \), until residues of \( \xi^{\sigma^{g-1}} \) are

\[ (\alpha_g, \beta_1, \ldots, \beta_{g-1}, \beta_g, \ldots, \alpha_{g-1}) \in \mathbb{F}_r^{2g}. \]

Define \( \pi = \prod_{i=0}^{g-1} \xi^{\sigma^{-i}} \). Then:

\( \pi \mod r = \prod_{i=1}^{g} \alpha_i \in \mathbb{F}_r \), and \( \pi \mod \bar{r} = \prod_{i=1}^{g} \beta_i \in \mathbb{F}_r. \)
Imposing the pairing-friendly conditions

- Given $\xi \in \mathcal{O}_K$ with residues $\alpha_i, \beta_i$, we construct $\pi$ with

$$\pi \mod r = \prod_{i=1}^{g} \alpha_i, \quad \pi \mod \bar{r} = \bar{\pi} \mod r = \prod_{i=1}^{g} \beta_i.$$

- Choose $\alpha_i, \beta_i$ in advance so that
  1. $\prod_{i=1}^{g} \alpha_i = 1$ in $\mathbb{F}_r$,
  2. $\prod_{i=1}^{g} \beta_i$ is a primitive $k$th root of unity in $\mathbb{F}_r$,

and construct $\xi$ via Chinese Remainder theorem.

- Then
  1. $\pi \equiv 1 \pmod{r}$, so $N_{K/\mathbb{Q}}(\pi - 1) \equiv 0 \pmod{r}$,
  2. $\Phi_k(\pi \bar{\pi}) \equiv 0 \pmod{r}$.

- Conclusion: if $q = \pi \bar{\pi} = N_{K/\mathbb{Q}}(\xi)$ is prime, then abelian varieties $A/\mathbb{F}_q$ with Frobenius $\pi$ have embedding degree $k$ with respect to a subgroup of order $r$.

- Use CM methods to construct $A/\mathbb{F}_q$ with Frobenius $\pi$. 
Generalizing the FSS Method (F.)

- FSS method with Galois $K$ leads to varieties with $\rho \approx 2g^2$.
- Apply Brezing-Weng idea: parametrize subgroup order $r$ as polynomial $r(x) \in \mathbb{Z}[x]$.
- Use decomposition of $r(x)$ in $K[x]$ to construct $\pi(x) \in K[x]$ with pairing-friendly properties modulo $r(x)$.
- For certain $x_0 \in \mathbb{Z}$, $\pi(x_0)$ is Frobenius element of an $A/\mathbb{F}_q$ that has embedding degree $k$ with respect to $r(x_0)$.
- $A$ can be constructed explicitly using CM methods.
- Can produce families with smaller $\rho$-values:
  - $g = 2$ best result: $\rho = 4$ for $k = 5$.
  - $g = 3$ best result: $\rho = 12$ for $k = 7$. 
An alternative method for $g = 2$

- Main idea: find $A$ that is simple over $\mathbb{F}_q$ but isogenous to $E \times E$ over $\mathbb{F}_{q^d}$ for small $d$.
- Can deduce conditions on Frobenius $\pi$ for $E$ that make $A/\mathbb{F}_q$ pairing-friendly.
- Use Cocks-Pinch type methods to construct a $\pi$ satisfying these conditions.
- Use CM method to find $j$-invariant of $E$, then find equation for $A$.
- Kawazoe-Takahashi: examples with $j(E) = 8000$.
  - Best result: $\rho = 3$ for $k = 24$.
- F.-Satoh: construction for general $E$.
  - Best result: $\rho = 8/3$ for $k = 9$. 
Summary: Pairing-Friendly Abelian Varieties

1. MNT Method:
   - Only 4 possible embedding degrees ($k = 3, 4, 6, 10$).
   - No generalization to higher dimension.
   - Good for constructing elliptic curves of prime order.
   - Curves are rare.

2. Cocks-Pinch Method:
   - Works for arbitrary embedding degree $k$.
   - Generalizes to higher dimensions.
   - Can’t construct varieties of prime order ($\rho \approx 2g^2$).
   - Many varieties possible, easy to specify bit sizes.

3. Brezing-Weng Method:
   - Works for many embedding degrees $k$.
   - Generalizes to higher dimensions.
   - Usually can’t construct varieties of prime order ($g < \rho < 2g^2$).
     - Exception: Barreto-Naehrig elliptic curves with $k = 12$.
   - Many varieties possible, easy to specify bit sizes.