Heuristics

on

pairing-friendly abelian varieties

joint work with David Gruenewald

John Boxall

john.boxall@unicaen.fr

Laboratoire de Mathématiques Nicolas Oresme, UFR Sciences, Université de Caen Basse-Normandie, 14032 CAEN cedex, France

ANR project SIMPATIC (SIM and PAiring Theory for Information and Communication security)

Bordeaux, March 4th 2014

Outline of the talk

The set-up

Basic ingredients

- $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ three groups of prime order r
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ a pairing (bilinear map, supposed non-trivial)
- $\mathbb{G}_1$, $\mathbb{G}_2$ additive notation, $\mathbb{G}_T$ multiplicative notation
- Fast computation of the group laws and of the pairing
- Security:
  - DL in $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ must be hard
  - Bilinear Diffie-Helman (BDH, given $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, xP, xQ, yP, yQ, zP, zQ, compute $e(P, Q)^{xyz}$) must be hard
  - No easily computed isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$ in either direction (so in particular $\mathbb{G}_1 \neq \mathbb{G}_2$).

- Often in practice, $\mathbb{G}_1$ and $\mathbb{G}_2$ groups of points on elliptic curves or abelian varieties, $\mathbb{G}_T$ group of roots of unity in a finite field
- In this talk: we discuss only this case

Notation and assumptions

- p prime, q a power of p
- $\mathbb{F}_q$ finite field of q elements (mostly $q = p$), $\mathbb{F}_p \subseteq \mathbb{F}_q$ prime field
- A abelian variety over $\mathbb{F}_q$
- $g = g_A = \dim A$
- $\mathbb{G}_1 \in A(\mathbb{F}_q)$ of order r
- for ease of computation, want q as small as possible with respect to r:
    - Weil bounds: $(\sqrt{q} - 1)^{2g} \leq \sharp A(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}$
    - $\implies$ ideally, r close to q^g
- rho-value $\rho := g \frac{\log q}{\log r}$.
    - $\implies \rho \geq 1$ and ideally, ρ close to 1
    - $\implies q = r^{\rho/g}$

- Security: DL in $\mathbb{F}_p(\boldsymbol{\mu}_r)$ ($\boldsymbol{\mu}_r$ = group of r^{th} of unity in $\overline{\mathbb{F}}_q$) must be hard
- Embedding degree: smallest integer $k \geq 1$ such that $\mathbb{F}_q(\boldsymbol{\mu}_r) = \mathbb{F}_{q^k}$.
- (Rubin -Silverberg): Under fairly general hypotheses: if $k \geq 2$ then $A(\mathbb{F}_{q^k})$ contains a subgroup $\mathbb{G}_2 \neq \mathbb{G}_1$ of order r such that there exists a fast computable pairing $\mathbb{G}_1 \times \mathbb{G}_2 \to \boldsymbol{\mu}_r$.
  - The proof gives $\mathbb{G}_2$ a trace 0 subgroup, so in general no easily computable isomorphism between $\mathbb{G}_2$ and $\mathbb{G}_1$.
- k must chosen so that
  - DL in $\mathbb{F}_p(\boldsymbol{\mu}_r)^\times$ to be hard (requires k sufficiently large)
  - computation in $\mathbb{F}_{q^k}$ as fast as possible (suggests k small)

Table adapted from Freeman-Scott-Teske:

Security level (bits)	r (bits)	q^k (bits)	$k\rho/g$
128	256	$3000 - 5000$	$12 - 20$
192	384	$8000 - 10000$	$20 - 26$
256	512	$14000 - 18000$	$28 - 36$

Examples:

- $g = 1$, $\rho = 1$, $\implies 12 \leq k \leq 20$: good for 128-bit level,
- $g = 2$, $\rho = 4$, $\implies 14 \leq k \leq 18$: good for 256-bit level.

Constructing the data

- q-Weil number: an algebraic integer all of whose complex conjugates satisfy $\pi\overline{\pi} = q$
- q-Weil polynomial: a monic polynomial in $\mathbb{Z}[x]$ all of whose roots are q-Weil numbers
- Two types of q-Weil numbers:
  - real: $\pi = q^{1/2}$ or $-q^{1/2}$ (degree one or two)
  - complex: $\mathbb{Q}(\pi)$ is a CM-field (a totally imaginary quadratic extension of a totally real field)

- (Honda-Tate): there is a bijection

$$\{\text{irreducible } q\text{-Weil polynomials}\} \Longleftrightarrow \{\text{isogeny classes of simple abelian varieties over } \mathbb{F}_q\}$$

- Warning: even if $\mathbb{Q}(\pi)$ is a CM-field, we may have dim(abelian variety) $\neq \frac{1}{2}[\mathbb{Q}(\pi) : \mathbb{Q}]$.
- (Waterhouse, Freeman-Stevenhagen-Streng): Let $g \geq 1$ and let p be a prime. Let π be a p-Weil number such that $\mathbb{Q}(\pi)$ is a CM-field of degree $2g$. Then the abelian varieties over $\mathbb{F}_p$ in the isogeny class corresponding to the minimal polynomial of π have dimension g. Furthermore, if p is unramified in $\mathbb{Q}(\pi)$, they are ordinary.

- Problem 1
  - k is the order of q in $(\mathbb{Z}/r\mathbb{Z})^\times$
  - but $(\mathbb{Z}/r\mathbb{Z})^\times$ is cyclic of order $r-1$, so random elements will have large order, much to large to be able to compute in $\mathbb{F}_{q^k}$.
  - so, random searching infeasible
- Want data (r, M, q) as follows
  - r divides $\Phi_k(q)$ (recall r prime, $\Phi_k = k^{\text{th}}$ cyclotomic polynomial)
  - M an irreducible q-Weil polynomial
  - r divides $M(1)$
  - rho-value $g\frac{\log q}{\log r}$ as close to 1 as possible
- Problem 2
  - how to find such data?
  - easy if one could factor $\Phi_k(q)$
  - impractical for crypographically useful examples
  - useful for searching for baby examples to test heuristics on distribution

- Problem 3. Given (r, M, q), need to be able to compute at least one abelian variety in the isogeny class corresponding to M.
  - CM methods ($g = 1$, 2)
  - theta functions
- purpose of talk: present heuristics on the distribution of data in certain cases of Problem 2, especially in the context of Freeman-Scott-Teske

Review of CM-types

- K CM-field of degree $2g$,
- $c : \mathbb{C} \to \mathbb{C}$ complex conjugation $c(z) = \overline{z}$
- CM-type on K: a set Φ of g embeddings $K \to \mathbb{C}$ such that $\mathrm{Hom}(K, \mathbb{C}) = \Phi \cup c \circ \Phi$ disjoint union (or the pair (K, Φ))
- CM-types (K, Φ) and (K', Φ') equivalent if there exists an isomorphism $\sigma : K \to K'$ and $\alpha \in \mathrm{Aut}(\mathbb{C})$ such that $\Phi' = \alpha \circ \Phi \circ \sigma^{-1}$.
- L a Galois closure of K, $\iota : L \to \mathbb{C}$ fixed embedding. If $F \subseteq L$, G_F subgroup of $G = \mathrm{Gal}(L/\mathbb{Q})$ fixing F.
  - Identify elements of Φ with embeddings of K in L using ι
  - $S = S_\Phi$ set of all elements of $\mathrm{Gal}(L/\mathbb{Q})$ whose restriction to K belongs to Φ.
- G_0 subgroup of Γ such that $\sigma \circ g \in S$ for all $\sigma \in S$, $g \in G_0$
- $G_K \subseteq G_0$: Φ primitive if $G_K = G_0$
- K_0 subfield of K corresponding to K_0; Φ primitive $\iff K_0 = K$

Reflex (dual) CM-type

- $S^{-1} = \{\sigma^{-1} \mid \sigma \in S\}$
- $G' = \{g \in G \mid \tau \circ g \in S^{-1} \text{ for all } \tau \in S^{-1}\}$
- $\hat{K}$ = subfield of L corresponding to G', so $G' = G_{\hat{K}}$
- $\hat{K}$ the reflex field of K, a CM-field
  - f symmetric function in the elements of Φ: $a \in K \Longrightarrow f(a) \in \hat{K}$
  - $\hat{K}$ generated over $\mathbb{Q}$ by elements of the form $\sum_{\phi \in \Phi} \phi(a)$, $a \in K$.
  - type norm $\mathrm{N}_\Phi : K^\times \to \hat{K}^\times$, $\mathrm{N}_\Phi(a) = \prod_{\phi \in \Phi} \phi(a)$
  - image of N_Φ contained in the subgroup $\{b \in \hat{K}^\times \mid b\bar{b} \in \mathbb{Q}\}$ of $\hat{K}^\times$
- $\hat{\Phi}$ the reflex CM-type of Φ: the set of embeddings $\hat{K} \to L$ (or $\hat{K} \to \mathbb{C}$) which are restrictions to $\hat{K}$ of elements of S^{-1}.
- $\hat{\Phi}$ always primitive
- if Φ is primitive, $\hat{\hat{K}} = K$ and $\hat{\hat{\Phi}} = \Phi$
- reflex type norm $\mathrm{N}_{\hat{\Phi}} : \hat{K}^\times \to K^\times$, $\mathrm{N}_{\hat{\Phi}}(b) = \prod_{\hat{\phi} \in \hat{\Phi}} \hat{\phi}(b)$

Examples

(Explicit description of one CM-type in each equivalence class):

- $g = 1$: K imaginary quadratic, 2 CM-types, equivalent, primitive
  - $K = L$, $\Phi = \hat{\Phi} = \{\mathrm{id}_K\}$
- $g = 2$: K quartic CM field, 4 CM-types
  - $K = L$, G a Klein four-group, 2 equivalence classes, neither primitive
    - K_1 and K_2 the two imaginary quadratic subfields of K
    - for $i = 1, 2$: $\Phi_i = G_{K_i}$, $K_0 = K_i = \hat{K}$, $\hat{\Phi}_i = \{\mathrm{id}_{K_i}\}$
  - $K = L$, G cyclic of order 4, 1 equivalence class, primitive
    - g a generator of G, $\Phi = \{\mathrm{id}_K, g\}$, $\hat{K} = K$, $\hat{\Phi} = \{\mathrm{id}_K, g^{-1}\}$
  - $K \neq L$, G dihedral of order 8, 1 equivalence class, primitive
    - g generator of G_K, M unique real quadratic subfield of L, h generator of G_M, $G =< g, h >$, $hg = gh^{-1}$
    - $\Phi = \{\mathrm{id}_K, h\}$, $\hat{K}$ defined by $G_{\hat{K}} = \{\mathrm{id}, hg\}$, $\hat{\Phi} = \{\mathrm{id}, g\}$

- $g = 3$: $[K : \mathbb{Q}] = 6$, 8 CM-types
  - K contains an imaginary quadratic subfield K_1 (necessarily unique): 2 equivalence classes, one primitive the other not
    - Non-primitive class: $K_0 = \hat{K} = K_1$, Φ a set of representatives of G_K/G_{K_1}, $\hat{\Phi} = \{\mathrm{id}_{K_1}\}$.
    - Either $K = L$ and G cyclic of order 6, or $K \neq L$ and G dihedral of order 12
    - Primitive class: g a generator of unique cyclic subgroup of G of order 6, $\Phi = \{\mathrm{id}, g, g^2\}$, $\hat{K} = K$, $\hat{\Phi} = \{\mathrm{id}, g^{-1}, g^{-2}\}$
  - K does not contain an imaginary quadratic subfield: 1 equivalence class, primitive
    - $K \neq L$, and G has order 24 or 48
    - In both cases: G has 4 Sylow-3 subgroups, all conjugate, $H = \{\mathrm{id}, h, h^2\}$ one of them: Φ = restriction of the elements of H to K
    - $\hat{K}$ given by $G_{\hat{K}} = H$ when $|G| = 24$, $G_{\hat{K}}$ = unique symmetric group S_3 containing H when $|G| = 48$
    - Note $[\hat{K} : \mathbb{Q}] = 8$
    - $\hat{\Phi}$ = set of distinct restrictions to $\hat{K}$ of the elements of G_K

p-Weil numbers and CM-types

- (K, Φ) a CM-type, $[K : \mathbb{Q}] = 2g$
- Recall reflex norm $\mathrm{N}_{\hat{\Phi}} : \hat{K}^{\times} \to K^{\times}$
- for all $b \in \hat{K}^{\times}$, $\mathrm{N}_{\hat{\Phi}}(b)\overline{\mathrm{N}_{\hat{\Phi}}(b)} \in \mathbb{Q}^{\times}$
- induces homomorphisms on ideal groups $\mathrm{N}_{\hat{\Phi}} : I(\hat{K}) \mapsto I(K)$ and ideal class groups $\mathrm{N}_{\hat{\Phi}} : Cl_{\hat{K}} \to Cl_K$
- $h_{\hat{K}}$ = order of $Cl_{\hat{K}}$
- Define $Cl(\hat{\Phi})$ to be the subgroup of $Cl_{\hat{K}}$ consisting of classes γ such that for all ideals $\mathfrak{A} \in \gamma$, $\mathrm{N}_{\hat{\Phi}}(\mathfrak{A})$ is principal and has a generator α such that $\alpha\overline{\alpha} \in \mathbb{Q}$
- $h_{\hat{\Phi}}$ = order of $Cl(\hat{\Phi})$

- From now on $q = p$ prime, π a p-Weil number in K
- Say π comes from Φ if there is a an ideal $\mathfrak{A} \in I(\hat{K})$ such that $\mathrm{N}_{\hat{\Phi}}(\mathfrak{A})$ is principal with generator π

Proposition

Let (K, Φ) be a CM-type, let p be a prime unramified in K and let $\pi \in K$ be a p-Weil number coming from Φ.
(i) There is a unique prime ideal $\mathfrak{P}$ of $\hat{K}$ such that π generates the ideal $\mathrm{N}_{\hat{\Phi}} \mathfrak{P}$ of K. Furthermore, $\mathfrak{P}$ is of degree one, and its ideal class belongs to $Cl(\hat{\Phi})$.
(ii) If (K, Φ) is primitive, then $K = \mathbb{Q}(\pi)$.

- w_K number of roots of unity in K

Theorem

Let Φ be a CM-type on K. Then the number $\pi_\Phi(x)$ of p-Weil numbers coming from Φ with p prime and $p \leq x$ is asymptotically equal to

$$\pi_\Phi(x) \sim \frac{w_K h_{\hat{\Phi}}}{h_{\hat{K}}} \int_2^x \frac{du}{\log u}$$

as $x \to \infty$.

- Proof easy, using (i) of the Proposition and the Prime Ideal Theorem in $\hat{K}$

Corollary

Let K be a CM-field. Then there exists a constant $C > 0$ such that the number $\pi_{K,\mathrm{Weil}}(x)$ of p-Weil numbers belonging to K with p prime and $p \leq x$ is asymptotically equal to

$$\pi_{K,\mathrm{Weil}}(x) \sim C \int_2^x \frac{du}{\log u}$$

as $x \to \infty$.

- C is rational
- Question: is there a simple formula for C in terms of invariants of K?

Heuristics for K fixed

- From now on, $q = p$ a prime only
- Motivation: want heuristics for the asymptotic behaviour as $x \to \infty$ of the number of data (r, M, p) as before, with
  - $g \geq 2$, K CM field of degree $2g$, $k \geq 2$ integer and $\rho_0 > 1$ real, all fixed
  - $r \leq x$ a prime
  - $p \leq r^{\rho_0/g}$
  - M irreducible p-Weil polynomial of degree $2g$ such that $\mathbb{Q}[x]/M(x) \simeq K$
  - r divides $\Phi_k(p)$
  - r divides $M(1)$
- Must have $\rho_0 \geq g/\varphi(k)$ (otherwise the conditions $p \leq r^{\rho_0/g}$ and r divides $\Phi_k(p)$ inconsistent)
- Freeman-Stevenhagen-Streng $\Longrightarrow$ such data correspond with finitely many exceptions to isogeny classes of pairing-friendly ordinary g-dimensional abelian varieties over prime fields

- Easier to work with triples (r, π, p) where π is a p-Weil number in K such that $K = \mathbb{Q}(\pi)$
- Each datum (r, M, p) corresponds to $|\mathrm{Aut}(K)|$ such triples
- Need to fix a CM-type Φ on K and consider only p-Weil numbers coming from Φ
- Using uniform distribution assumptions about the congruence classes of p-Weil numbers modulo prime ideals of K dividing r, together with the Theorem, one is led to the following

- Recall notation:
  - w_K number of roots of unity in K, $h_{\hat{K}}$ class number of $\hat{K}$, $h_{\hat{\Phi}}$ order of class group $Cl(\hat{\Phi})$ as above
  - $e(k, K)$ degree of $\mathbb{Q}(\zeta_k) \cap K$ over $\mathbb{Q}$ (where $\mathbb{Q}(\zeta_k)$ is the k^{th} cyclotomic field)

Fixed K heuristic estimate

Let $g \geq 2$, $k \geq 2$ be integers, and let $\rho_0 > \max(1, \frac{g}{\varphi(k)})$ be a real number such that $\rho_0 \neq g$. Fix a CM-field K of degree $2g$, a CM-type Φ on K and let $e(k, K)$, w_K, $h_{\hat{K}}$ and $h_{\hat{\Phi}}$ be as above. Then the number of triples (r, π, p) as above with $r \leq x$ and $p \leq r^{\frac{\rho_0}{g}}$ that come from Φ is equivalent as $x \to \infty$ to

$$\frac{e(k, K) g w_K h_{\hat{\Phi}}}{\rho_0 h_{\hat{K}}} \int_2^x \frac{du}{u^{2-\frac{\rho_0}{g}} (\log u)^2}$$

- Works also when $g = 1$, provided $k \geq 3$ and $K \neq \mathbb{Q}(\zeta_k)$
- When Φ is primitive, by (ii) of the Proposition all but finitely many p-Weil numbers π coming from Φ satisfy $K = \mathbb{Q}(\pi)$, so get estimate for number of isogeny classes of ordinary-pairing friendly abelian varieties A with $\mathrm{End}(A) \otimes \mathbb{Q} \simeq K$ and Frobenius π coming from Φ.
- The integral converges if and only if $\rho_0 \leq g$
  - expect only finitely many triples if $\rho_0 < g$
  - exclude boundary case $\rho_0 = g$

Effect of polynomial families

- Construction of Brezing-Weng, Freeman-Scott-Teske when $g = 1$, Freeman in general
- $r_0(u) \in \mathbb{Z}[u]$, $p_0(u) \in \mathbb{Q}[u]$, $\pi_0(u) \in K[u]$ such that
    - $p_0(u)$ is irreducible and $\pi_0(u)\overline{\pi}_0(u) = p_0(u)$
    - $r_0(u)$ is irreducible with positive leading coefficient and $\mathbb{Q}[u]/r_0(u)$ contains a subfield isomorphic to K
    - $r_0(u)$ divides $\Phi_k(p_0(u))$ and $\mathrm{N}_{K/\mathbb{Q}}(\pi_0(u) - 1)$
    - there exist integers $h \geq 1$, u_0 such that $\frac{r_0(u_0)}{h} \in \mathbb{Z}$, $p(u_0) \in \mathbb{Z}$ and

$$\gcd\left\{\frac{r_0(u_0)p(u_0)}{h} \;\middle|\; u_0, \frac{r_0(u_0)}{h}, p(u_0) \in \mathbb{Z}\right\} = 1$$

- Under these conditions, it is conjectured that there are infinitely many $u_0 \in \mathbb{Z}$ such that $\frac{r_0(u_0)}{h}$ and $p_0(u_0)$ are simultaneously prime, so that $\pi_0(u_0)$ is a $p_0(u_0)$-Weil number in K
- If so, get infinite set of data $(\frac{r_0(u_0)}{h}, M_{u_0}, p_0(u_0))$, where M_{u_0} minimal polynomial of $\pi_0(u_0)$

- As u_0 grows, the rho-value $\frac{g \log p_0(u_0)}{\log(r_0(u_0)/h)}$ approaches $g\frac{\deg(p_0)}{\deg(r_0)}$
- Define $g\frac{\deg(p_0)}{\deg(r_0)}$ to be the ρ-value of the polynomial family
- Precise heuristic asymptotic formula for the number $\mathcal{N}(X)$ of u_0 with $|u_0| \leq X$ such that $\frac{r_0(u_0)}{h}$ and $p_0(u_0)$ simultaneously prime (Bateman-Horn, K. Conrad):

$$\mathcal{N}(X) \sim C\frac{X}{(\log(X))^2}$$

  where $C > 0$ depends only on $r_0(u)$ and $p_0(u)$
- Deduce that if

$$g\frac{\deg(p_0)}{\deg(r_0)} < \rho_0 < g\Big(1 + \frac{1}{\deg(r_0)}\Big),$$

  the polynomial family will produce more triples (r, π, p) then predicted by the K fixed heuristic estimate

- Only known example of this:
- $g = 1$, $k = 12$, $K = \mathbb{Q}(\sqrt{-3})$, the Barreto-Naehrig family:
  - $r_0(u) = 36u^4 + 36u^3 + 18u^2 + 6u + 1$, $\pi_0(u) = \frac{t_0(u)+y_0(u)\sqrt{-3}}{2}$, where

$$t_0(u) = 6u^2 + 1, \qquad y_0(u) = 6u^2 + 4u + 1$$

  - So, Bateman-Horn predicts more data than fixed K heuristic estimate when $1 < \rho_0 < 1.25$
  - Data seems consistent with idea that the fixed K heuristic estimate predicts asymptotically the number of data not belonging to the Barreto-Naehrig family

Numerical data (K fixed)

- $g = 1$
  - easy, since p-Weil numbers are just generators of principal prime ideals of degree one,
  - the formulae simplify, since $\hat{K} = K$ is imaginary quadratic and $cl(\hat{\Phi}) = \{1\}$
  - number of triples (r, π, p) with $r \leq x$, $p \leq r^{\rho_0}$, $\pi\overline{\pi}$ expected to be asympototic to
$$\frac{e(k,K)w_K}{\rho_0 h_K}\int_2^x \frac{du}{u^{2-\rho_0}(\log u)^2}$$
  - boring, since apart from obvious constraints like $r \equiv 1 \pmod{k}$ and r splits in K, there seems no way of counting data other than checking all possible values of $r \leq x$, $p \leq r^{\rho_0}$ one-by-one
  - at most a couple of minutes on a laptop suffices to produce meaningful data for given k, K (say $r \leq 2 \times 10^8$)

- $g \geq 2$
  - in practice $g = 2$ or $g = 3$, one example with $g = 4$
  - need to determine, for each p, whether there exists a p-Weil number in K (and whether it comes from Φ, though this is not a problem in cases where there is only one equivalence class of primitive CM-types)
    - factorize p in K and make a list $D(p)$ of all decompositions $p\mathcal{O}_K = \mathfrak{a}\overline{\mathfrak{a}}$
    - ignore those decompositions that come from proper CM subfields pf K
    - test whether $\mathfrak{a}$ is principal and if so, find a generator γ
    - test whether the unit η such that $\gamma\overline{\gamma} = p\eta$ is of the form $\varepsilon\overline{\varepsilon}$
    - if so, $\pi := \frac{\gamma}{\varepsilon}$ is a p-Weil number generating $\mathfrak{a}$, and every p-Weil number generating $\mathfrak{a}$ is of the form $\omega\pi$ for some root of unity ω in K
  - some p can be eliminated by congruence considerations, which imply that $D(p)$ must be empty; especially if the maximal abelian subfield M of L or $M \cap K$ is large
  - need from 40 minutes to several hours to obtain meaningful data for given k, K

Presentation of the data

- $N(k, K, \rho_0, (a, b))$, the number of data corresponding to isogeny classes of pairing-friendly abelian varieties with $a \leq r \leq b$
- $I = I(k, K, \rho_0, (a, b))$ predicted value, i. e.

$$I = \frac{e(k, K) g w_K h_{\hat{\Phi}}}{|\mathrm{Aut}(K)| \rho_0 h_{\hat{K}}} \int_a^b \frac{du}{u^{2-\frac{\rho_0}{g}} (\log u)^2}$$

Example with $g = 2$, G cyclic

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	I	$k=8$	$k=24$	I	$k=16$	$k=32$	I
2.8	2	3	1	0	0	0	1.02	7	1	2.03	3	4	4.07
2.9	4	3	2	0	3	1	1.74	8	1	3.48	7	5	6.97
3.0	8	3	6	1	5	2	3.00	16	3	6.00	10	11	11.99
3.1	14	5	8	2	10	3	5.18	20	5	10.36	22	17	20.73
3.2	22	9	9	6	13	5	8.99	23	15	17.98	43	33	35.96
3.3	30	14	15	12	26	14	15.66	36	30	31.31	63	58	62.62
3.4	46	27	26	23	40	31	27.37	61	55	54.73	112	104	109.46
3.5	68	51	59	38	59	49	48.00	99	110	96.00	178	187	192.00

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}[X]/(X^4 + 4X^2 + 2)$.

Invariants: $w_K = 2$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, G cyclic.

Example with $g = 2$, G cyclic

ρ_0	$k=2$	$k=3$	$k=4$	$k=12$	$k=24$	$k=36$	I	$k=5$	$k=10$	$k=15$	$k=20$	$k=25$	I
2.5	0	3	0	2	2	2	1.04	2	4	9	2	4	4.15
2.6	2	3	2	3	2	6	1.75	6	10	12	3	6	7.01
2.7	2	5	2	3	4	7	2.98	10	22	17	5	6	11.91
2.8	2	6	2	6	6	10	5.08	14	26	29	14	9	20.33
2.9	6	9	8	8	9	10	8.71	26	46	45	32	22	34.84
3.0	10	15	14	18	17	18	14.99	64	70	72	49	51	59.97
3.1	16	27	20	32	24	27	25.91	106	124	125	83	93	103.63
3.2	26	44	43	52	35	50	44.95	176	168	210	150	162	179.79
3.3	70	76	72	82	72	87	78.28	302	302	335	282	319	313.12
3.4	112	142	140	143	130	141	136.83	574	560	597	534	578	547.30
3.5	212	250	241	258	235	251	240.00	1000	1000	1049	977	1006	959.99

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}(\zeta_5)$.

Invariants: $w_K = 10$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, G cyclic.

Example with $g = 2$, G dihedral

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	I	$k=12$	$k=24$	$k=36$	I
2.7	2	0	0	1	2	2	1.19	2	2	2	2.38
2.8	2	2	2	4	3	3	2.03	2	4	6	4.07
2.9	6	5	3	6	3	4	3.48	8	8	9	6.97
3.0	6	8	6	10	6	7	6.00	17	14	11	11.99
3.1	8	13	11	11	10	14	10.36	25	25	17	20.73
3.2	16	23	19	20	17	25	17.98	44	43	36	35.96
3.3	32	31	26	34	27	39	31.31	65	71	64	62.62
3.4	58	59	56	57	54	66	54.73	116	116	115	109.46
3.5	100	97	93	93	96	117	96.00	206	195	191	192.00

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}[X]/(X^4 + 8X^2 + 13)$.

Invariants: $w_K = 2$, $h_{\hat{\Phi}} = h_{\hat{K}} = 2$, G dihedral.

Example with $g = 3$, G cyclic

ρ_0	$k=2$	$k=4$	$k=5$	I	$k=3$	$k=6$	I	$k=9$	$k=18$	I
4.0	6	3	0	2.99	2	4	5.99	22	18	17.97
4.1	8	6	2	4.27	6	8	8.54	34	24	25.62
4.2	10	6	6	6.10	10	18	12.20	46	44	36.60
4.3	14	10	8	8.73	14	22	17.46	64	54	52.38
4.4	16	11	13	12.52	20	30	25.04	82	72	75.13
4.5	24	15	23	17.99	30	38	35.98	124	116	107.94
4.6	32	24	30	25.90	50	62	51.79	180	160	155.37
4.7	44	34	42	37.34	80	80	74.68	260	236	224.05
4.8	68	51	62	53.94	114	116	107.88	390	330	323.63
4.9	90	71	82	78.04	166	162	156.09	568	454	468.27
5.0	136	104	114	113.11	250	224	226.22	812	658	678.66
5.1	224	169	159	164.19	380	328	328.38	1238	944	985.15

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}(\zeta_9)$.

Invariants: $w_K = 18$, $h_{\hat{\Phi}} = h_{\hat{K}} = 1$, G cyclic.

Example with $g = 3$, G of order 12

ρ_0	$k=2$	$k=4$	$k=5$	$k=32$	l	$k=3$	$k=6$	$k=24$	l
3.9	0	3	0	0	1.05	2	4	3	2.10
4.0	0	3	0	0	1.50	2	4	5	2.99
4.1	0	3	0	1	2.13	4	6	7	4.27
4.2	2	3	0	2	3.05	6	6	10	6.10
4.3	4	5	0	4	4.37	8	6	15	8.73
4.4	6	5	2	6	6.26	14	8	21	12.52
4.5	12	8	6	9	9.00	20	14	32	17.99
4.6	16	12	9	13	12.95	22	24	53	25.90
4.7	22	15	13	20	18.67	32	34	67	37.34
4.8	40	23	24	30	26.97	44	50	84	53.94
4.9	50	35	32	42	39.02	62	80	119	78.04
5.0	64	52	57	58	56.55	110	118	160	113.11
5.1	88	74	96	84	82.10	164	170	214	164.19

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}[X]/(X^6 + 24X^4 + 144X^2 + 27)$.

Invariants: $w_K = 6$, $h_{\hat{\Phi}} = 1$, $h_{\hat{K}} = 2$, G of order 12.

Example with $g = 3$, $|G| = 24$

ρ_0	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	I	$k=7$	$k=14$	$k=35$	I
4.4	0	2	0	2	3	1.04	5	2	4	3.13
4.5	0	2	0	2	4	1.50	10	4	4	4.50
4.6	2	2	0	3	5	2.16	11	5	6	6.47
4.7	2	3	0	4	6	3.11	15	7	10	9.34
4.8	2	6	3	6	8	4.49	16	14	11	13.48
4.9	2	8	4	8	8	6.50	23	23	17	19.51
5.0	8	13	6	15	10	9.43	37	37	25	28.28
5.1	12	14	9	18	14	13.68	48	49	40	41.05

Values of $N(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for $K = \mathbb{Q}[X]/(X^6 + 35X^4 + 364X^2 + 1183)$.

Invariants: $w_K = 2$, $h_{\hat{\Phi}} = 4$, $h_{\hat{K}} = 16$, G of order 24.

Example with $g = 4$, $|G| = 24$

	$k=4$		$k=5$		heuristic	$k=3$		$k=6$		heuristic
ρ_0	N_{Φ_6}	N_{Φ_8}	N_{Φ_6}	N_{Φ_8}	$I_{\Phi_6} = I_{\Phi_8}$	N_{Φ_6}	N_{Φ_8}	N_{Φ_6}	N_{Φ_8}	$I_{\Phi_6} = I_{\Phi_8}$
6.0	5	9	16	12	9.00	16	20	18	14	18.00
6.1	6	11	18	19	11.82	20	24	26	20	23.64
6.2	12	14	21	26	15.54	30	28	36	28	31.09
6.3	21	25	27	32	20.47	42	38	56	38	40.93
6.4	31	39	32	37	26.97	56	62	74	50	53.94
6.5	40	51	41	46	35.57	68	74	94	62	71.15
6.6	49	64	53	55	46.96	90	96	128	82	93.94
6.7	62	81	74	72	62.07	136	130	152	116	124.14
6.8	85	104	89	94	82.10	176	176	196	152	164.19
6.9	117	133	118	131	108.68	240	216	236	222	217.36
7.0	157	167	159	171	144.00	300	286	300	314	288.00

Two inequivalent primitive CM types, Φ_6 with $[\hat{K} : \mathbb{Q}] = 6$ and Φ_8 with $\hat{K} = K$

Values of $N_{\Phi_i}(k, K, \rho_0, (10^4, 5 \cdot 10^5))$ for the field

$$K = \mathbb{Q}[X]/(X^8 + 78X^6 + 1323X^4 + 7401X^2 + 9801).$$

Invariants: $w_K = 6$, $h_{\hat{\Phi}_6} = 4, h_{\hat{K}_6} = 8$, $h_{\hat{\Phi}_8} = 2, h_{\hat{K}_8} = 4$.

Heuristics with fixed maximal real subfield

- Wanted ρ close to one, but K fixed heuristic estimate suggests we can expect infinitely many examples only when $\rho_0 > g$
- So, what happens if K is allowed to vary?
- We suppose K_0^+ is a totally real field and look at triples (r, π, p) with $K_0^+(\pi)$ quadratic over K_0^+
- $(x - \pi)(x - \overline{\pi}) = x^2 - \tau x + p$ with every real conjugate of τ satisfying $|\tau| \leq 2\sqrt{p}$, and conversely such (p, τ) give rise to p-Weil numbers π and $\overline{\pi}$
- d_0 discriminant of K_0^+
- As $X \to \infty$, the number of algebraic integers $\tau \in K_0^+$ all of whose real conjugates satisfy $|\tau| \leq X$ is asymptotically equivalent to $(2X)^g d_0^{-1/2}$

- Using this, asymptotics of sums of the form $\sum_{p \leq U, p \text{ prime}} p^{\alpha}$ and hypotheses of uniform distribution of Weil numbers π modulo ideals dividing r, we obtain

Fixed K_0^+ heuristic estimate

Let $g \geq 1$, $k \geq 2$ be integers with $(g,k) \neq (1,2)$, let K_0^+ be a totally real field of degree g and let $\rho_0 > \max(1, \frac{g}{\varphi(k)})$ be a real number with $\rho_0 \neq \frac{2g}{g+2}$. Then the number $R(k, K_0^+, \rho_0, x)$ of triples (r, π, p) with $[K_0^+(\pi) : K_0^+] \leq 2$ and $r \leq x$ satisfies as $x \to \infty$

$$R(k, K_0^+, \rho_0, x) \sim \frac{g 4^{g+1} e(k, K_0^+)}{\rho_0 (g+2) d_0^{1/2}} \int_2^x \frac{u^{\rho_0\left(\frac{1}{2}+\frac{1}{g}\right)-2} du}{(\log u)^2}.$$

Here d_0 denotes the discriminant of K_0^+ and $e(k, K_0^+)$ the degree of $K_0^+ \cap \mathbb{Q}(\zeta_k)$ over $\mathbb{Q}$.

- Expect $R(k, K_0^+, \rho_0, x)$ to tend to infinity with x for all $\rho_0 > \max(1, \frac{g}{\varphi(k)})$ when $g = 2$ but not when $g > 2$
- Can compute $R(k, K_0^+, \rho_0, x)$ as follows
  - if $r \leq x$, for every real conjugate of τ: $|\tau| \leq 2\sqrt{p} \leq 2x^{\frac{\rho_0}{2g}}$
  - make a list $\mathcal{L}$ of all integers $\tau \in K_0^+$ all of whose conjugates satisfy $|\tau| \leq 2x^{\frac{\rho_0}{2g}}$
  - for each $\tau \in \mathcal{L}$, factor $\Phi_k(\tau - 1)$ into prime ideals in K_0^+ and make a list $\mathcal{M}(\tau)$ of all degree one primes $\mathfrak{r}^+$ dividing $\Phi_k(\tau - 1)$ of norm r such that $x \geq r \geq (\frac{|\tau|}{2})^{\frac{2g}{\rho_0}}$ for every real conjugate of τ
  - for each $\mathfrak{r}^+ \in \mathcal{M}(\tau)$, search for primes $p \leq x^{\frac{\rho_0}{g}}$ such that $p \equiv \tau - 1 \pmod{\mathfrak{r}^+}$ and $|\tau| \leq 2\sqrt{p}$ for every real conjugate of τ
- Problem: need to factor $\Phi_k(\tau - 1)$ in K_0^+
- Hence: only works for k with $\varphi(k)$ small
- On the other hand: when ρ_0 small, we diminish the number of cases to consider

Presentation of the data

- $R_c(k, K_0^+, \rho_0, (a, b))$ expected number of data (r, M, p) corresponding to isogeny classes of pairing-friendly abelian varieties with $a \leq r \leq b$ (so $R_c = R/|\mathrm{Aut}(K_0^+)|$)
- $J = J(k, K_0^+, \rho_0, (a, b))$ predicted value, i. e.

$$J = \frac{g 4^{g+1} e(k, K_0^+)}{|\mathrm{Aut}(K_0^+)| \rho_0 (g+2) d_0^{1/2}} \int_a^b \frac{u^{\rho_0\left(\frac{1}{2}+\frac{1}{g}\right)-2} du}{(\log u)^2}$$

k	3	4	5	6	7	8	9	10	11	12	13	14
R_k	440	395	496	521	515	445	467	487	538	514	516	459

k	15	16	17	18	19	20	21	22	23	24	25	26
R_k	460	453	443	460	513	457	458	486	477	477	460	462

k	27	28	29	30	31	32	33	34	35	36	37	38
R_k	506	521	441	530	486	467	494	518	480	466	471	514

k	39	40	41	42	43	44	45	46	47	48	49	50
R_k	510	523	472	478	459	427	459	454	479	478	497	482

Values of $R_k = R_c(k, \mathbb{Q}, 1.1, (10^8 - 2 \times 10^7, 10^8 + 2 \times 10^7))$ for $3 \leq k \leq 50$

Note: $J = J(k, \mathbb{Q}, 1.1, (10^8 - 2 \times 10^7, 10^8 + 2 \times 10^7)) \approx 455.0$ for all $k \geq 3$

ρ_0	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=12$	J	$k=8$	J
1.0	1	0	0	0	0	1	0.16	0	0.33
1.1	1	0	0	1	0	1	0.36	0	0.73
1.2	2	0	0	1	2	2	0.83	1	1.65
1.3	4	1	0	1	3	3	1.92	1	3.85
1.4	7	2	5	5	4	6	4.59	7	9.18
1.5	15	11	14	15	12	17	11.21	22	22.42
1.6	36	22	28	34	25	37	27.95	62	55.90
1.7	81	68	62	88	62	80	71.04	157	142.09
1.8	200	194	192	219	161	210	183.80	384	367.60
1.9	493	518	467	496	534	543	483.16	940	966.33
2.0	1346	1418	1267	1331	1295	1321	1288.45	2572	2576.91

Values of $R_c(k, K_0^+, \rho_0, (10^3, 10^5))$ for $K_0^+ = \mathbb{Q}(\sqrt{2})$.

d	$k=3$	$k=4$	$k=5$	$k=6$	$k=12$	J	d	$k=3$	$k=4$	$k=5$	$k=6$	$k=12$	J
2	1346	1418	1267	1331	1321	1288.45	26	365	408	368	374	358	357.35
3	1144	1093	1049	1103	2199	1052.02	29	675	718	688	662	660	676.73
5	1650	1808	3306	1670	1703	1629.78	30	356	338	322	346	354	332.68
6	789	794	774	753	751	743.89	31	351	351	333	345	328	327.27
7	755	718	634	667	708	688.71	33	643	687	621	664	640	634.39
10	659	635	573	599	616	576.21	34	325	324	336	287	291	312.50
11	574	580	534	553	567	549.40	35	319	341	285	311	349	308.00
13	1090	1043	1064	975	1084	1010.75	37	634	596	654	614	609	599.12
14	521	526	494	491	432	486.99	38	309	320	299	313	302	295.59
15	486	460	487	443	475	470.48	39	325	334	280	307	306	291.78
17	967	954	952	880	902	883.87	41	609	651	580	537	602	569.14
19	422	480	450	395	412	418.03	42	320	280	316	303	255	281.16
21	883	753	799	798	810	795.25	43	302	300	296	274	300	277.88
22	396	415	405	379	414	388.48	46	307	289	258	300	253	268.66
23	377	393	418	378	396	379.94	47	273	258	311	257	252	265.79

Values of $R_c(k, \mathbb{Q}(\sqrt{d}), 2.0, (10^3, 10^5))$ for $k \in \{3,4,5,6,12\}$ and $d \leq 50$ squarefree.

Entries in red show the cases where $e(k, \mathbb{Q}(\sqrt{d})) = 2$. Otherwise $e(k, \mathbb{Q}(\sqrt{d})) = 1$

ρ_0	$k=3$	$k=4$	$k=5$	$k=6$	J	$k=7$	J
1.5	3	0	1	0	0.65	2	1.96
1.6	3	0	1	1	1.20	2	3.60
1.7	10	11	1	3	2.22	6	6.66
1.8	10	11	1	5	4.14	9	12.41
1.9	10	28	1	9	7.75	24	23.26
2.0	18	42	1	15	14.61	30	43.84
2.1	32	53	12	35	27.70	77	83.10
2.2	144	82	40	68	52.78	230	158.33
2.3	197	82	97	160	101.05	324	303.15
2.4	244	232	97	236	194.37	716	583.11
2.5	354	519	280	362	375.53	1028	1126.60
2.6	557	1048	714	865	728.59	1647	2185.76
2.7	1211	1654	1314	1132	1419.19	3267	4257.58
2.8	2474	3050	2640	1598	2774.87	9820	8324.62
2.9	5136	5527	5330	3993	5445.06	19124	16335.18
3.0	9378	10116	8179	11699	10721.16	35287	32163.49

Values of $R_c(k, K_0^+, \rho_0, (10^3, 10^4))$ for $K_0^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

When g gets large

- As g grows, the condition $p \leq r^{\frac{\rho_0}{g}}$, becomes more and more restrictive
- therefore get few values of r and p, and lots of τ's with all real conjugates $|\tau| \leq 2\sqrt{p}$
- for r, p fixed: as τ varies, the roots π and $\overline{\pi}$ of $x^2 - \tau x + p$ generate different CM fields with maximal real subfield equal to K_0^+

THANK YOU FOR YOUR ATTENTION!