# Finding optimal elliptic curves for high-security pairings

Craig Costello

craig.costello@qut.edu.au

talk based on...

C-Lauter-Naehrig'11: Attractive subfamilies of BLS curves for implementing high-security pairings
C'12 (in submission): Particularly friendly members of family trees (2012/072)

June 21, 2012

# What's a pairing

A pairing is a **bilinear** map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$
$$P \times Q \longmapsto e(P, Q)$$

- **Bilinear:** $\mathbf{e([a]P, [b]Q) = e(P, Q)^{ab} = e([b]P, [a]Q)}$
- $\mathbb{G}_1$ and $\mathbb{G}_2$ are (prime) order $r$ groups on an elliptic curve $E/\mathbb{F}_q$
- $\mathbb{G}_T$ is the order $r$ multiplicative group of the extension field $\mathbb{F}_{q^k}$
- All three discrete log problems need to be intractable
- $r$ large, $q^k$ much larger again
- The *embedding degree* $k \in \mathbb{Z}$ plays a vital role in pairing-based cryptography

# Example: $P \in E(\mathbb{F}_q)$, $Q \cong Q' \in E(\mathbb{F}_{q^2})$, $e(P, Q) \in \mathbb{F}_{q^{12}}$

$$P=\left(664072627004787196566504964561727344070428369705\ ,1458656105509069348006973843968312782707543657947\right)$$

$$Q=\Big(\ (794912935384259695643941666982448931339755393931i + 1292183349923355671495373600673278028719609109506)z^2$$

$$,(451143164328155547079674992688956153701248999656i + 1245161133325846984203018563019795198131589273628)z^3\Big)$$

$$e(P, Q)=$$

$$(137233103417929071753763396884161306211453124856 1i + 3173430919531087423273025324263589125596227361 50)z^5 +$$

$$(657494535236813609177311808779244063930185280957i + 1173891693415235640893762327708485517080457926012)z^4 +$$

$$(750659053186983976728590236941743928841799248238i + 7888755765082195399211117059098672821757403215 93)z^3 +$$

$$(134265911670016233313286840340328675010513764877 1i + 4006734067447289466903829837505406075197246452 84)z^2 +$$

$$(200064485727654206845371455070977617286564943382i + 3153560672118122820083723590769338263346755137 54)z +$$

$$184511804126153037736870425849119616499303527350i + 5953241769845308475576662965641401256198925473 93$$

# Example: $P \in E(\mathbb{F}_q)$, $Q' \in E(\mathbb{F}_{q^2})$, $e([a]P, Q) \in \mathbb{F}_{q^{12}}$

$$[a]P = \left(66407262700478719656650496456172734407042836970 5 , 145865610550906934800697384396831278270754365794 7\right)$$

$$Q = \left( (794912935384259695643941666982448931339755393931i + 129218334992335567149537360067327802871960910950 6)z^2 \right.$$

$$\left. , (451143164328155547079674992688956153701248999656i + 124516113332584698420301856301979519813158927362 8)z^3 \right)$$

$$e(P, Q)^a =$$

$$(303440764161389278186025527562206061259856205015i + 985347885483078762431227918897173021282189858464)z^5 +$$

$$(510834944292113049952437630800572365012238607403i + 358877166719808056705221690966131424851586311 7)z^4 +$$

$$(841156839227960247262828400536345831531061869301i + 279940199499261423258814782923099552018529421 73)z^3 +$$

$$(351425148932022687391429784471978558159619833853i + 106301923135750601336194578170356475880798183822 2)z^2 +$$

$$(108436361699674247600295475429010290800276735073 2i + 763775041639272282778383398061688619679620899 64)z +$$

$$548988961733999661302517240851774796430896571032i + 385042254582483177311552059176916929021740844169$$

# Example: $P \in E(\mathbb{F}_q)$, $Q' \in E(\mathbb{F}_{q^2})$, $e([a]P, [b]Q) \in \mathbb{F}_{q^{12}}$

$$[a]P = \Big(664072627004787196566504964561727344070428369705\ ,1458656105509069348006973843968312782707543657947\Big)$$

$$[b]Q = \Big($$

$$(7949129353842596956439416669824489313397553939 31i + 1292183349923355671495373600673278028719609109506)z^2$$

$$,(4511431643281555470796749926889561537012489996 56i + 1245161133325846984203018563019795198131589273628)z^3\Big)$$

$$e(P,Q)^{ab} =$$

$$(2597883896869293288674272869671235493234475696 11i + 1306674915064924383001093696143033943265614307882)z^5 +$$

$$(3348399645546177193304959039997328836114829778 62i + 1432529381150637754170708881340020431629734575924)z^4 +$$

$$(7025651716397085899356441515989294934269419251 41i + 4182194279284545288287863626216133209724936588 22)z^3 +$$

$$(6137954750788369515303608684980716078511520640 51i + 1382644658025115080479255569216265441954127694835)z^2 +$$

$$(9880194899461493435756144731893608413102897196 7i + 8398467052063193110051158117646094425184827890 10)z +$$

$$1333332858144207093683795787968513598183630940508i + 1604413125696705854321957038005484407706684394 05$$

# Pairing-friendly curves

**Definition: $E$ is a pairing-friendly curve if...**

- $k$ is small (less than 50)
- the prime $r$ dividing $\#E$ has $\rho = \frac{\log_2 q}{\log_2 r} \leq 2$

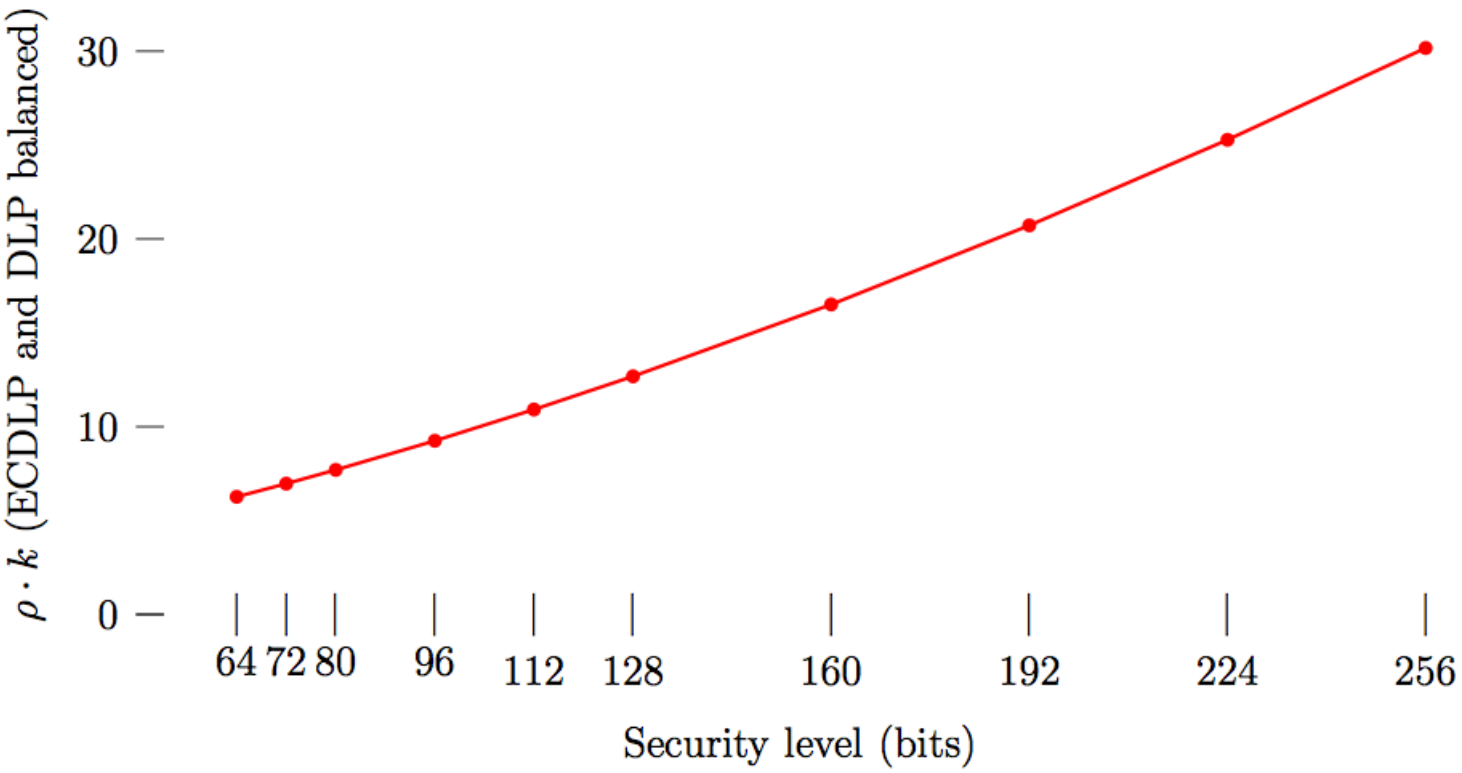
- $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ defined over $\mathbb{F}_{q^k}$ iff
$$r \mid q^k - 1$$
- Group order can lie anywhere between...
$$q - \lfloor 2\sqrt{q} \rfloor = 146150162449679026514546172069156880588098716010$$
$$q = 146150162449679026514544858992078549371725889081 9$$
$$q + \lfloor 2\sqrt{q} \rfloor = 146150162449679026514551007772414106846419065628$$
- $r = \#E =$146150162449679026514547380994971188499300027613
- ... then think of $r$ and $q$ as independent of each other
- $k$ being small enough is extremely unlikely in general
- **Moral of the story: pairing-friendly curves are very rare**

# The Barreto-Naehrig (BN) family

'05

- in our example...
  $q = 146150162449679026514544858992078549371725889081 9$
  $\#\mathrm{E} =$
  $r = 146150162449679026514544738099497118849930002761 3$
- parameters come from putting $x = 448873741399$ into
  $$q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$
  $$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$
- Guaranteed that $k = 12$
- Notice $\rho = 1$ (perfect), also curves are always $y^2 = x^3 + b$

# Balancing security requires varied $k$



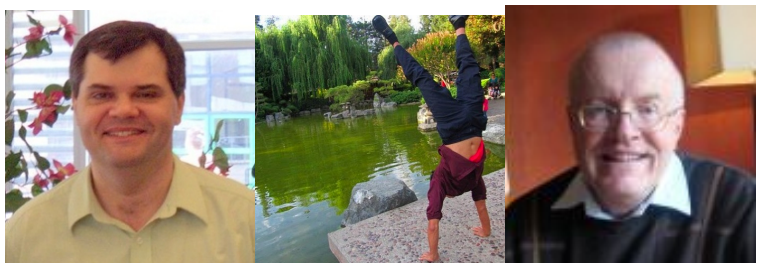

Example - a BN $k = 12$ ($\rho = 1$) curve:
Perfect for the 128-bit security level: $r \approx 256$-bits, $q^{12} \approx 3072$-bits.

`http://www.keylength.com/en/3/`

`http://www.fujitsu.com/global/news/pr/archives/month/2012/20120618-01.html`

# Other complete (popular) families

- $k = 12, 24, 27, 48$ Barreto-Lynn-Scott (BLS) families



- $k = 16, 18, 32, 36$ Kachisa-Schaefer-Scott (KSS) families

- e.g. the $k = 48$ BLS family: $x \equiv 1 \bmod 3$ $(y^2 = x^3 + b)$

$$q(x) = (x-1)^2(x^{16} - x^8 + 1)/3 + x;$$

$$n(x) = (x-1)^2(x^{16} - x^8 + 1)/3 \qquad r(x) = x^{16} - x^8 + 1.$$

- e.g. the $k = 16$ KSS family: $x \equiv \pm 25 \bmod 70$ $(y^2 = x^3 + ax)$

$$q(x) = (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125)/980;$$

$$n(x) = (x^2 + 2x + 5)(x^8 + 48x^4 + 625)/980; \qquad r(x) = x^8 + 48x^4 + 625.$$

# Towered extension field arithmetic

- Koblitz-Menezes'05: for $k = 2^i 3^j$, build extension field as a sequence of quadratic and cubic subextensions (preferably binomials)
  - Karatsuba-like tricks make arithmetic much faster
  - easier to implement
  - twisted subfields constructed inherently
- e.g. a $k = 12$ tower

$$\mathbb{F}_q \xrightarrow{\beta^2-\alpha} \mathbb{F}_{q^2} \xrightarrow{\gamma^3-\beta} \mathbb{F}_{q^6} \xrightarrow{\delta^2-\gamma} \mathbb{F}_{q^{12}}.$$

- Instead of $\mathbb{F}_{q^{12}}$ multiplications costing 144 $\mathbb{F}_q$ multiplications, they cost $3 \cdot 3 \cdot 6 = 54$ $\mathbb{F}_q$ multiplications
- **Finding a nice (efficient) tower is not always possible**

# Parameterised families of pairing-friendly curves

- BLS curves with $k = 24$:

$$q(x) = (x-1)^2(x^8 - x^4 + 1)/3 + x;$$
$$n(x) = (x-1)^2(x^8 - x^4 + 1)/3;$$
$$r(x) = x^8 - x^4 + 1;$$

- when $q = q(x)$, $r = r(x)$ are prime, guaranteed a curve $E/\mathbb{F}_q : y^2 = x^3 + b$ with $r \mid n = \#E$.

- "perfect" for 256-bit security $\rho \cdot k = 30$ ($\rho = 1.25$)

# Example: searching for BLS curves

$$q(x) = (x-1)^2(x^8 - x^4 + 1)/3 + x; \qquad r(x) = x^8 - x^4 + 1.$$

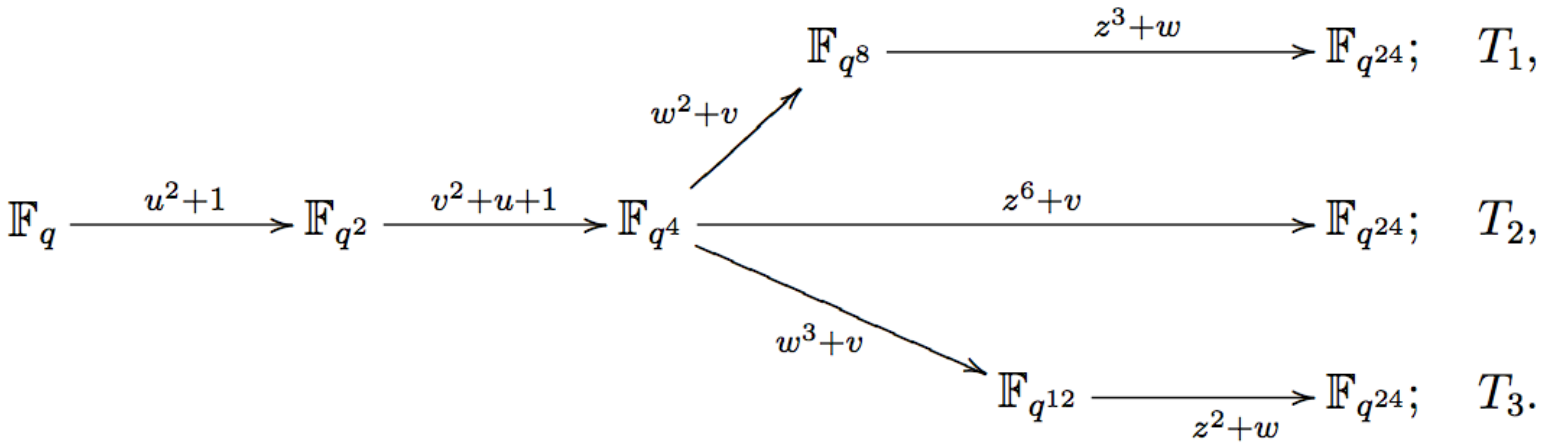
- Kick-start with $x = 2^{64} = 18446744073709551616$ (targeting 256-bit security): $x \equiv 1 \bmod 3$, $x \leftarrow x + 3$
- soon enough $x = 1844674407370956\,3373$
  $q =$
  152081353920740809892727066524584946339781036330218959281772305234001103872205207355200355585054305961029358887567446121016058918174051639618221302567689792185243234190430804646778679690996022143059610293588875674461210160589181740516396182213025676897921852432341904308046467786796909960221
- soon after $x = 1844674407370956\,8134$
  $q =$
  152081353920741202406074204344187845907416165206148514542547681060676871445712171751406826067585894672662267520862173865039526651345269582899549251926695033086714461488802549208755951847449677789467266226752086217386503952665134526958289954925192669503308671446148880254920875595184744967777
- **moral: thousands/millions/billions... of possible curves to choose from...**
- (also) primality testing at high-security levels takes time...

# Attractive subfamilies of BLS curves for high-security

## Theorem (C-Lauter-Naehrig'11)

*Instead of* $x \equiv 1 \bmod 3$, *take*

| $x_0$ mod 72 | $q(x_0)$ mod 72 | $n(x_0)$ mod 72 | *efficient tower* | *curve* $E$ | *correct twist* $E'$ |
|---|---|---|---|---|---|
| **7** | *19* | *12* | ✓ | $y^2 = x^3 + 1$ | $y^2 = x^3 \pm 1/v$ |
| **16** | *19* | *3* | ✓ | $y^2 = x^3 + 4$ | $y^2 = x^3 \pm 4v$ |
| **31** | *43* | *12* | ✓ | $y^2 = x^3 + 1$ | $y^2 = x^3 \pm v$ |
| **64** | *19* | *27* | ✓ | $y^2 = x^3 - 2$ | $y^2 = x^3 \pm 2/v$ |



# Particularly friendly members of family trees

- Most recent work took this "subfamilies" idea further
- Thoroughly explored the other 8 families of interest: BW $k = 8$, BLS $k = 12$, KSS $k = 16$, KSS $k = 18$, BLS $k = 27$, KSS $k = 32$, KSS $k = 36$, BLS $k = 48$
- Two (quartic/sextic) twist types: type $M$ and type $D$ (type $D$ previously preferred - untwisting isomorphism)... but **CLN'10 Theorem remedies this!**: there is no preference
- Also give compact generators for many of the favoured subfamilies

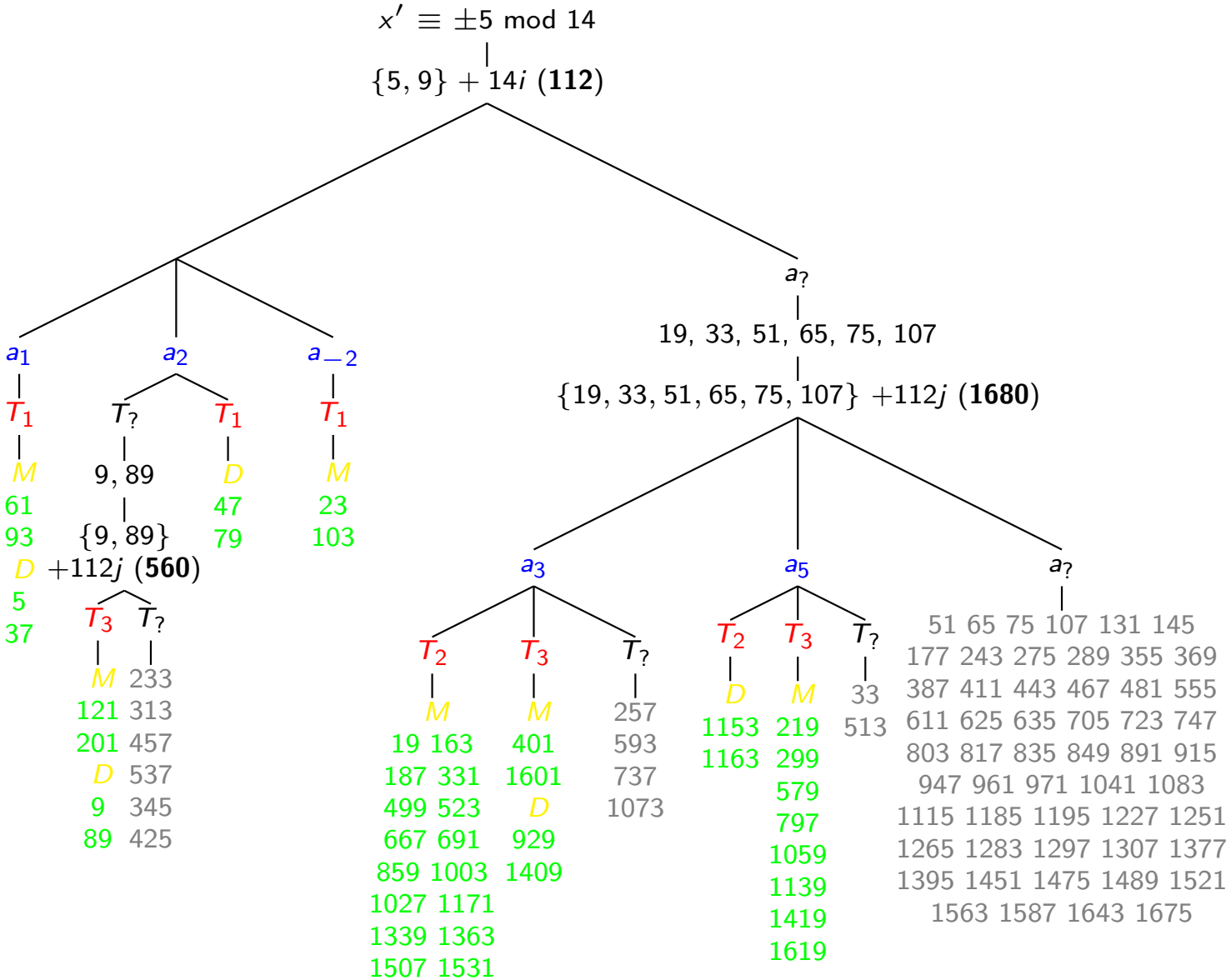



Figure: Example: The $k = 16$ KSS family tree.

# Picking fruits from the trees: e.g. $k = 16$ tree

| $\mathbb{F}_p \xrightarrow{\mathbb{F}_p[u]/(u^2+u_i)} \mathbb{F}_{p^2} \xrightarrow{\mathbb{F}_{p^2}[v]/(u^8-v_i)} \mathbb{F}_{p^{16}}$ | | | |
|---|---|---|---|
| $T_i$ | $T_1$ | $T_2$ | $T_3$ |
| $(u_i, v_i)$ | $(2, u)$ | $(3, u)$ | $(5, u)$ |

Table: Efficient towering options in the $k = 16$ KSS tree.

| rating | equiv. class for $x'$ ($x' = x/5$) | tower | $a$ | twist type | $\mathbb{G}_1$ gen. $[h](\cdot,\cdot)$ | $\mathbb{G}_2'$ gen. $[h']( \cdot, \cdot)$ | % |
|---|---|---|---|---|---|---|---|
| | $61, 93 \bmod 112$ | $T_1$ | 1 | $M$ | - | $\left(v-1, \sqrt{(v-1)^3 + v(v-1)}\right)$ | 12.2 |
| | $5, 37 \bmod 112$ | $T_1$ | 1 | $D$ | - | $\left(-v, \sqrt{-v^3-1}\right)$ | 12.7 |
| $\star\star\star\star\star$ | $47, 79 \bmod 112$ | $T_1$ | 2 | $D$ | - | $\left(2/v, \sqrt{\frac{8}{v^3} + \frac{4}{v^2}}\right)$ | 12.1 |
| | $23, 103 \bmod 112$ | $T_1$ | $-2$ | $M$ | $(1, \sqrt{-1})$ | - | 13.1 |
| $\star\star\star\star$ | $\{19, \ldots, 1531\}_{16} \bmod 1680$ | $T_2$ | 3 | $M$ | $(1, 2)$ | $\left(3/v, \sqrt{\frac{27}{v^3} + \frac{9}{v^2}}\right)$ | 7.9 |
| $\star\star\star$ | $1153, 1633 \bmod 1680$ | $T_2$ | 5 | $D$ | $\left(2, 2\sqrt{3}\right)$ | - | 0.9 |

- Implementors can use our trees to tailor-make searches that target specific parameter combinations/preferences
- good searches will only search low-hamming weight $x$-values
- ... or choose from our extensive list (low hamming-weight examples)