Pairing-Friendly Hyperelliptic Curves

Laura Hitt

The University of Texas at Austin,

now at University College Dublin

11th Workshop on Elliptic Curve Cryptography 2007

Shannon Institute, September 6, 2007

Outline

- Background of hyperelliptic curve, pairing-based cryptography
- Mathematical framework
- Cryptographic parameters
- Pairing-friendly curves
- Family of pairing-friendly curves of genus 2

Hyperelliptic Curve Cryptography

- 1989–Koblitz proposed hyperelliptic curves and the associated Jacobian variety, J_C, to supply the group.
- There is ongoing “conversation" about using elliptic vs. hyperelliptic curves...

  See Tanja and Dan’s series of talks at ECC 2006, 2007...

Why HECC?

Security is related to difficulty of solving the DLP in a (sub)group of large prime order...

With $g > 1$, it is possible to work over a smaller field while achieving the same group size as with elliptic curves.

- For genus 1 curves over $\mathbb{F}_q$, need $q > 2^{160}$.
- For genus 2, can have $q \approx 2^{80}$; genus 3, $q \approx 2^{54}$.

What is a pairing?

A pairing is a map

$$e : G_1 \times G_1' \longrightarrow G_2$$

where G_1, G_1', G_2 are groups of order r, such that the following hold:

- bilinear: $e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab}$
- non-degenerate: for every $P \in G_1, P \neq 0$, there exists $Q \in G_1'$ such that $e(P, Q) \neq 1$.

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing
  - Frey-Rück attack–uses Tate pairing

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
    - MOV attack–uses Weil pairing
    - Frey-Rück attack–uses Tate pairing
- Constructive:

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing
  - Frey-Rück attack–uses Tate pairing
- Constructive:
  - One-round three person key agreement

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing
  - Frey-Rück attack–uses Tate pairing
- Constructive:
  - One-round three person key agreement
  - Identity-based encryption

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing
  - Frey-Rück attack–uses Tate pairing
- Constructive:
  - One-round three person key agreement
  - Identity-based encryption
  - Short digital signatures

Pairing-based Cryptography

- Destructive: transport the DLP from the curve to a finite field, where there are more efficient methods for solving the DLP.
  - MOV attack–uses Weil pairing
  - Frey-Rück attack–uses Tate pairing
- Constructive:
  - One-round three person key agreement
  - Identity-based encryption
  - Short digital signatures
  - And more!

    (Sakai, Ohgishi, Kasahara, Joux, Boneh, Franklin,...)

Curves for Pairings

What curves do we use?

- For general (hyper)elliptic curve cryptography, somewhat “randomly" generated curves can be used.

  But...

- For pairing-based systems, certain properties are required for the curves, such as:
  - embedding degree k–want "small enough"
  - security indicator k'–want "large enough"

Pairing-friendly Curves

- $\#J_C(\mathbb{F}_q)$ divisible by a large prime r so the DLP in the r-order subgroup is resistant to known attacks.
  - prime $r > 2^{160}$
- Minimal embedding field large enough so that the DLP in it withstands index-calculus attacks.
  - $q^{k'} > 2^{1024}$
- Embedding degree k small enough for the pairing over $\mathbb{F}_{q^k}$ to be efficiently computable.
  - say $2 \leq k \leq 30g$

Mathematical Framework

- Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements.
- A **hyperelliptic curve** C **of genus** g **over** $\mathbb{F}_q$ is defined by a non-singular equation of the form

$$C : y^2 + h(x)y = f(x),$$

where $h, f \in \mathbb{F}_q[x], \deg(f) = 2g + 1, \deg(h) \leq g, f$ monic, $g > 0 \in \mathbb{Z}$.

When $g = 1$ we call C an **elliptic curve**.

Mathematical Framework

- If E is an elliptic curve, then the set of $\mathbb{F}_q$-rational points, $E(\mathbb{F}_q)$, forms a group.
- For hyperelliptic curves with $g \geq 2$, must use the group of $\mathbb{F}_q$-rational points (divisors) of the **Jacobian of** C.
  - The Jacobian of C, J_C, is an abelian variety of dimension g such that

$$J_C(\mathbb{F}_q) \backsimeq \mathrm{Pic}^0_{\mathrm{C}}(\mathbb{F}_q)$$

where $\mathrm{Pic}^0_{\mathrm{C}}(\mathbb{F}_q) = \mathrm{Div}^0_{\mathrm{C}}(\mathbb{F}_q)/\mathrm{Princ}_C(\mathbb{F}_q)$, the degree zero divisor class group of C over $\mathbb{F}_q$.

Mathematical Framework

- **Theorem**: $(\sqrt{q}-1)^{2g} \le \#J_C(\mathbb{F}_q) \le (\sqrt{q}+1)^{2g}$.
  - So $\#J_C(\mathbb{F}_q) \sim q^g$ when q is large compared to g.
- For $g \ge 2$, one can work over a smaller $\mathbb{F}_q$ and yet achieve a group of similar size to that of an elliptic curve.

Mathematical Framework

- $J_C(\mathbb{F}_q)[r]$ denotes the set of r**-torsion points** of $J_C(\mathbb{F}_q)$, i.e. all $P \in J_C(\mathbb{F}_q)$ such that $[r]P = O$.
- When over a field of characteristic $p > 0$, J_C is said to have p**-rank** s if the subgroup of points of order p (over $\overline{\mathbb{F}_q}$) has cardinality p^s.

Mathematical Framework

- $J_C(\mathbb{F}_q)[r]$ denotes the set of r**-torsion points** of $J_C(\mathbb{F}_q)$, i.e. all $P \in J_C(\mathbb{F}_q)$ such that $[r]P = O$.
- When over a field of characteristic $p > 0$, J_C is said to have p**-rank** s if the subgroup of points of order p (over $\overline{\mathbb{F}_q}$) has cardinality p^s.
  - C is **ordinary** if J_C has p-rank g;

Mathematical Framework

- $J_C(\mathbb{F}_q)[r]$ denotes the set of r**-torsion points** of $J_C(\mathbb{F}_q)$, i.e. all $P \in J_C(\mathbb{F}_q)$ such that $[r]P = O$.
- When over a field of characteristic $p > 0$, J_C is said to have p**-rank** s if the subgroup of points of order p (over $\overline{\mathbb{F}_q}$) has cardinality p^s.
  - C is **ordinary** if J_C has p-rank g;
  - C is **supersingular** if J_C is isogenous over $\overline{\mathbb{F}_q}$ to the product of supersingular elliptic curves (an elliptic curve is **supersingular** if it has p-rank 0).

Pairings

Let r be a large prime dividing $\#J_C(\mathbb{F}_q)$, coprime to q, and μ_r be the r-th roots of unity.

We have the Weil pairing, Tate pairing, eta pairing, ate pairing...

The **reduced Tate pairing** is a bilinear non-degenerate map

$$t_r : J_C(\mathbb{F}_{q^k})[r] \times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k}) \longrightarrow \mu_r$$

where

$$t_r(P, Q) = f_P(D_Q)^{(q^k-1)/r}.$$

These pairings can be computed using a generalization of Miller's algorithm.

Embedding Degree k

- Traditionally, the pairings were viewed as mapping the DLP into the smallest extension of $\mathbb{F}_q$ containing μ_r. That is, $\mathbb{F}_q(\mu_r) = \mathbb{F}_{q^k}$ for some integer k.
- The degree of this extension was called the **embedding degree** $\mathbf{k}$.
  So k is the smallest positive integer such that $r \mid q^k - 1$.
- Thus the security of a DL cryptosystem has been understood to be related to the size of k. (Galbraith suggests k/g.)

Minimal Embedding Field

Galbraith and Rubin-Silverberg recognized an exception:

> In the supersingular case it is possible for the minimal embedding field to be $\mathbb{F}_{q^{k/2}}$.

We will show that if $q = p^m$ for $m > 1$, then

- the difference in the field exponents of $\mathbb{F}_{q^k}$ and the minimal embedding field can be as much as a factor of m.
- this includes the non-supersingular case as well.

Implications

Since it may be possible for pairings to embed into a significantly smaller field than $\mathbb{F}_{q^k}$, we note that:

- Attacks on the DLP can be dramatically faster than expected.
- There may exist curves used in DL systems that are not as secure as believed.
- A modified parameter needs to be used to indicate security.

Minimal Embedding Field

Let a be a positive integer, r a prime, $r \nmid a$.
The *order of* a *modulo* r, denoted by $\mathrm{ord}_{\mathbf{r}}\mathbf{a}$, is the smallest positive integer x such that $a^x \equiv 1 \bmod r$.

Lemma 0.1. Let $q = p^m$ for some prime p and positive integer m, r be a prime not equal to p, and k be the smallest integer such that $q^k \equiv 1 \bmod r$. Then

$$k = \frac{\mathrm{ord}_r p}{\gcd(\mathrm{ord}_r p, m)}.$$

Minimal Embedding Field

- When q is not prime, the minimal embedding field is
$$\mathbb{F}_{p^{\mathrm{ord}_r p}} = \mathbb{F}_{p^{kD}},$$
where $D = \gcd(\mathrm{ord}_r p, m)$.

- It suffices to have a positive **rational** number k', not merely an integer k, with $q^{k'} - 1$ divisible by the prime r.
  - $k' = \frac{\mathrm{ord}_r p}{m}$
  - The minimal embedding field is $\mathbb{F}_{q^{k'}}$.

Field Diagram

$$\begin{tikzcd}
& \mathbb{F}_{q^k} \arrow[dl, dash, "k"'] \arrow[dd, dash, "\geq 1"] \\
\mathbb{F}_q \arrow[dd, dash, "m"'] & \\
& \mathbb{F}_{q^{k'}} = \mathbb{F}_{q^{\mathrm{ord}_r p/m}} = \mathbb{F}_{p^{kD}} \\
\mathbb{F}_p \arrow[ur, dash, "\mathrm{ord}_r p"'] &
\end{tikzcd}$$

where $D = \gcd(\mathrm{ord}_r p, m)$

Examples

Example 0.1. Let $r = 2^p - 1$ be prime, and $q = 2^{p+s}$, for integer $1 \leq s \leq p+1,\ s \neq p$.

For each s, there exists at least one non-supersingular elliptic curve over $\mathbb{F}_q$ with $|E(\mathbb{F}_q)| = 2^s r$.

- These curves have embedding degree $k = p$, so $\mathbb{F}_{q^k} = \mathbb{F}_{2^{p(p+s)}}$.
- But $\gcd(\mathrm{ord}_r 2, p+s) = 1$, so the minimal embedding field is $\mathbb{F}_{2^p}$, and these extension degrees differ by a factor of $\Delta = p + s$.

Examples (preprint Galbraith, McKee, Valença)

Example 0.2. Family of (ordinary) genus 2 curves over $\mathbb{F}_q$ where $q(l) = l^2$ for any prime (power) l. The associated Jacobian has size $n(l) = l^4 \pm l^3 + l^2 \pm l + 1$.

- These curves have embedding degree $k = 5$.
- However, if $n(l) = l^4 + l^3 + l^2 + l + 1$, then prime r dividing $n(l)$ also divides $l^5 - 1 = q^{5/2} - 1$, so in fact the minimal embedding field cannot be larger than $\mathbb{F}_{q^{5/2}}$.
- Dramatic difference in how large l must be chosen for curve to remain secure; curve may have been such that $q^5 > 2^{1024}$, but probably wasn't checked for $q^{5/2} > 2^{1024}$.

Examples

Example 0.3. The genus 2 curve over $\mathbb{F}_{2^{267}}$ given by the characteristic polynomial of Frobenius with coefficients $(a_1, a_2) = (-1, 2^{267} + 2^{178})$. Then $\#J_C(\mathbb{F}_{2^{267}}) = 2^{178} \cdot 17 \cdot r$, where $r = \frac{2^{4(89)}+1}{17}$ is prime.

- The embedding degree is $k = 8$.
- Since $\log_2 r = 351$ and $k \log_2 q = 2136$, we have a 351-bit DLP on the curve, and a 2136-bit DLP in $\mathbb{F}^*_{q^k}$, which is considered hard.
- However, since $\mathrm{ord}_r 2 = 712$, then in the minimal embedding field we have only a 712-bit DLP, which is considered easy.

Examples

Example 0.4. The genus 2 curve over $\mathbb{F}_{2^{136}}$ given by the characteristic polynomial of Frobenius with coefficients $(a_1, a_2) = (-1, 2^{136} + 2^{124})$. Then $\#J_C(\mathbb{F}_{2^{136}}) = 2^{124} \cdot 17 \cdot r$, where $r = \frac{2^{4(37)}+1}{17}$ is prime.

- The embedding degree is $k = 37$.
- Since $k \log_2 q = 5032$, we have a 5032-bit DLP in $\mathbb{F}_{q^k}^*$, which is considered hard.
- However, since $\mathrm{ord}_r 2 = 296$, then in the minimal embedding field we have only a 296-bit DLP, which is considered easy.

Security Indicator

Solving the DLP *both* on the (Jacobian of the) curve and in the finite field containing the embedding, $\mathbb{F}_{q^{k'}}$, should be computationally infeasible.

Compare the size of the minimal embedding field with size of $J_C(\mathbb{F}_q)$:

$$\frac{\log p^{\mathrm{ord}_r p}}{\log q^g} = \frac{\mathrm{ord}_r p}{mg} = \frac{k'}{g}.$$

Security Indicator k'/g

Thus a security indicator should be k'/g, where $k' = \frac{\mathrm{ord}_r p}{m}$.

- Need to adjust standards specifications to consider the minimal embedding field.
  - In particular for non-supersingular elliptic curves over binary fields...

Security Standards

The *MOV condition* is checked when validating parameters for elliptic curves over binary fields.

- IEEE P1363: MOV condition "ensures that an elliptic curve is not vulnerable to the reduction attack of Menezes, Okamoto and Vanstone."
- For a field size q and base point order r, algorithm verifies $q^i \not\equiv 1 \bmod r$ for any $i \leq B$, where B is a selected *MOV threshold*.

Security Standards

We suggest appropriate modifications be made in the standards to account for the minimal embedding field.

- Check what we call the *subfield-adjusted MOV condition*:

  For field size $q = p^m$ and base point order r, $p^i \not\equiv 1 \bmod r$ for any $i \leq mB$.

See H. ePrint $2007 \backslash 343$.

Sizes for Security

One wants discrete logarithms in $\mathbb{F}_{q^{k'}}$ to be of approximate difficulty as elliptic curve discrete logarithms over $\mathbb{F}_q$.

So if we have a (sub)group of order r, and r is a 160-bit prime, then one would like

$$\boxed{q^{k'} > 2^{1024}.}$$

Minimal Embedding Field Summary

- Pairings embed into μ_r which lies in $\mathbb{F}_{p^{\mathrm{ord}_r p}} = \mathbb{F}_{q^{k'}}$ where $k' = \frac{\mathrm{ord}_r p}{m}$.
- Conceivable for the extension degree of this field to differ by a factor of m from that of $\mathbb{F}_{q^k}$.
- Critical to check when working over fields of small characteristic; if $q = p$, no discrepancy occurs.
- Use 2 parameters: embedding degree k for computations; $\frac{k'}{g}$ as a security indicator.
- Modify standards (such as IEEE P1363).

Parameter ρ

- It is desirable for $\#J_C(\mathbb{F}_q)$ to be prime or near-prime, to avoid known attacks.
- One examines the ratio $\rho = \frac{g \log_2 q}{\log_2 r}$.
- For secure and efficient implementation, the ideal situation is to have $\rho \sim 1$,

  Currently the best ratio achieved is $\rho \sim 5/4$, by Brezing and Weng.

Pairing-friendly Curves

- $\#J_C(\mathbb{F}_q)$ divisible by a large prime r so the DLP in the r-order subgroup is resistant to known attacks.
  - prime $r > 2^{160}$
- Minimal embedding field large enough so that the DLP in it withstands index-calculus attacks.
  - $q^{k'} > 2^{1024}$
- Embedding degree k small enough for the pairing over $\mathbb{F}_{q^k}$ to be efficiently computable.
  - say $2 \leq k \leq 30g$

Size of k

In general, k is enormous. However:

- Supersingular elliptic curves have $k \leq 6$.
  - In characteristic 2, we have $k \leq 4$.
  - In characteristic 3, we have $k \leq 6$.
  - Over prime characteristic $\mathbb{F}_p$ with $p \geq 5$, we have $k \leq 2$.

While we'd like k to be small, we'd like the flexibility of making k larger for more security, if needed.

So we try higher genus and/or non-supersingular curves.

Size of k

- Supersingular curves of genus 2 have $k \leq 12$.
- Ordinary genus 1 and genus 2 curves *in special cases* can achieve various $k \leq 12$.

Size of k

- Supersingular curves of genus 2 have $k \leq 12$.
- Ordinary genus 1 and genus 2 curves *in special cases* can achieve various $k \leq 12$.

  - We will focus on non-supersingular, non-ordinary hyperelliptic curves of genus 2.

Size of k

- Supersingular curves of genus 2 have $k \leq 12$.
- Ordinary genus 1 and genus 2 curves *in special cases* can achieve various $k \leq 12$.

  - We will focus on non-supersingular, non-ordinary hyperelliptic curves of genus 2.
  - We will give a family of such curves with small embedding degree (e.g. k=8,13,16).

Pairing-Friendly $g = 1$

Use CM methods to construct ordinary elliptic curves:

- Miyaji-Nakabayashi-Takano (2001)
- Cocks-Pinch (2001)
- Barreto-Lynn-Scott (2002)
- Galbraith-McKee-Valença (2004)
- Dupont-Enge-Morain (2005)
- Brezing-Weng (2005)
- Barreto-Naehrig (2005)
- Freeman (2006)

  See Freeman-Scott-Teske's “A Taxonomy of Pairing-Friendly Elliptic Curves"

Pairing-friendly $g = 2$

- Galbraith-McKee-Valença (2004)
- Hitt (2007)
- Freeman (2007)

Pairing-Friendly $g = 2$

- Galbraith-McKee-Valença (2004)–ordinary curves
- Hitt (2007)–2-rank 1 curves

Give families of non-supersingular hyperelliptic curves with small embedding degree.
Downfall: No explicit curve construction (only represent isogeny classes of Jacobians by characteristic polynomial of Frobenius).

- Freeman (2007)–ordinary curves

Constructs individual curves over prime fields (following Cocks-Pinch method, using CM).

Downfall: $\rho \sim 8$ too large for practical implementation.

Complex Multiplication Method for Elliptic Curves

For a given square-free $D > 0$, construct an elliptic curve E with CM by $\mathbb{Q}(\sqrt{-D})$.

- Fix D, k, find t, r, q satisfying:
  - r prime, q prime (or prime power),
  - $r \mid q + 1 - t$ (so $E(\mathbb{F}_q)$ has an r-order subgroup),
  - $r \mid q^k - 1$ and $r \nmid q^i - 1$ for $1 \leq i < k$ (so embedding degree k),
  - $Dy^2 = 4q - t^2$ for some integer y (called the CM equation).
- Find a root j of the Hilbert class polynomial $H_D(z)$; j is the j-invariant of a curve $E(\mathbb{F}_q)$.

Curves of Genus 2

- Freeman:
  - Find primes q, r and characteristic poly'l of Frobenius $h(x)$ of ordinary curve over $\mathbb{F}_q$ with embedding degree k.
  - Construct curve using roots of Igusa class polynomials for the quartic CM field $K = \mathbb{Q}[x]/(h(x))$.
- Galbraith, et al: Let $\Phi_k(x)$ be the k-th cyclotomic polynomial.
  - Parametrize quadratic $q(l)$ such that $\Phi_k(q(l))$ splits as $n_1(l)n_2(l)$.
  - Represent quadratic families by the characteristic polynomial of Frobenius of the ordinary curve over $\mathbb{F}_q$.
  - Unable to generate any curves using the CM method.

Our Approach

- Give a parametrization of a family of large integers $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ for $r \geq 0$ and odd $L \geq 5$.
- Determine the embedding degrees for subgroups having these orders when they are prime, and for various $\mathbb{F}_q$.
- Associate with each prime a sequence of genus 2 curves over $\mathbb{F}_q$, such that $N_{r,L} \mid \#J_C(\mathbb{F}_q)$.
- The $\mathbb{F}_q$-isogeny class of the Jacobian of C is determined by the characteristic polynomial of Frobenius.

Mathematical Framework

- In particular, for $g = 2$ there exist integers a_1, a_2 such that the characteristic polynomial of Frobenius is

$$f_{J_C}(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2,$$

where the a_1 and a_2 determine the $\mathbb{F}_q$-isogeny class of J_C.

- $\#J_C(\mathbb{F}_q) = 1 + a_1 + a_2 + q a_1 + q^2.$

Heuristics

$N_{r,L}$ will be of the form $\frac{A^L+1}{A+1}$ where L is prime and A is a positive integer.

If the behavior follows that of the primes $\frac{A^L-1}{A-1}$ and there is no algebraic factorization, then we would expect:

- infinitely many such primes,
- the number of such primes with $L \leq M$ is asymptotic to $\frac{\log\log M}{\log A}$ for fixed A.

Experimental evidence seems to confirm this for $r = 0, 2, 3$.

The Setup

Let $q = 2^m$ and C be a genus 2 curve over $\mathbb{F}_q$ of the form

$$y^2 + xy = ax^5 + bx^3 + cx^2 + dx$$

where $a \neq 0, b, c, d$ arbitrary.

- C is 2-rank 1.
- We will identify C by the (a_1, a_2), which determine the $\mathbb{F}_q$-isogeny class of the Jacobian.

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

- **Lemma 0.1.** Let $q = 2^m$, where $1 \leq m \leq 2^r(L-1)-1$, and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$. Then

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

- **Lemma 0.1.** Let $q = 2^m$, where $1 \leq m \leq 2^r(L-1) - 1$, and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$. Then
  - $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i L$ for $i \in \{0, \ldots, r-1\}$,

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

- **Lemma 0.1.** Let $q = 2^m$, where $1 \leq m \leq 2^r(L-1)-1$, and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$. Then
  - $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i L$ for $i \in \{0, \ldots, r-1\}$,
  - $k = 2^{r+1-i} L$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i$ for $i \in \{0, \ldots, r+1\}$.

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

- **Lemma 0.1.** Let $q = 2^m$, where $1 \leq m \leq 2^r(L-1) - 1$, and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$. Then
  - $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i L$ for $i \in \{0, \ldots, r-1\}$,
  - $k = 2^{r+1-i} L$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i$ for $i \in \{0, \ldots, r+1\}$.

    - k is always “small": $k < (\log\ q)^2$ for $L \geq 15$.

Family of Primes

Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be prime for $r \geq 0$, odd $L \geq 5$.

- **Lemma 0.1.** Let $q = 2^m$, where $1 \leq m \leq 2^r(L-1)-1$, and also allow $m = \frac{L+1}{2}$ in the case that $r = 0$. Then
  - $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i L$ for $i \in \{0, \ldots, r-1\}$,
  - $k = 2^{r+1-i} L$ when $\gcd(\mathrm{ord}_{N_{r,L}} 2, m) = 2^i$ for $i \in \{0, \ldots, r+1\}$.

    - k is always “small": $k < (\log\ q)^2$ for $L \geq 15$.
    - $k \leq ?$

Genus 2 Curves

Theorem 0.6. [Maisner and Nart] There exists a curve of the form $y^2 + xy = ax^5 + bx^3 + cx^2 + dx$, $a \neq 0, b, c, d$ arbitrary, with characteristic polynomial of Frobenius $f(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2$ if the following hold:

1. a_1 is odd
2. $|a_1| \leq 4\sqrt{q}$
3. (a) $2|a_1|\sqrt{q} - 2q \leq a_2 \leq a_1^2/4 + 2q$

   (b) a_2 is divisible by $2^{\lceil m/2 \rceil}$

   (c) $\Delta = a_1^2 - 4a_2 + 8q$ is not a square in $\mathbb{Z}$

   (d) $\delta = (a_2 + 2q)^2 - 4qa_1^2$ is not a square in $\mathbb{Z}_2$ (the 2-adic integers).

Proposition

Proposition 0.7. For odd $L \geq 9$, the following a_1 and a_2 satisfy the conditions for the existence of the genus 2 curves in the theorem of Maisner and Nart.

- When $m = \frac{L+1}{2}$, let $(a_1, a_2) = (1, -2^m)$.
- When $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, let $(a_1, a_2) = (-1, 2^m + 2^{2m-2^r L})$.

Main Theorem

Theorem 0.8. Let $N_{r,L} = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be a prime for some $r \geq 0$ and odd $L \geq 9$.

- If $r = 0$, then for $m = \frac{L+1}{2}$ there exists a genus 2 curve over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2 \cdot 3 \cdot N_{0,L}$, and $a_1 = 1, a_2 = -2^m$.

- If $r \geq 0$, then for each integer m in the interval $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1) - 1$, there exists a genus 2 curve over $\mathbb{F}_{2^m}$ with the property that $\#J_C(\mathbb{F}_{2^m}) = 2^x(2^{2^r}+1)N_{r,L}$, where $x = 2m - 2^r L$, and $a_1 = -1, a_2 = 2^m + 2^x$.

Parameter $\rho = \frac{g \log_2 q}{\log_2 N}$

For this family of curves, we have $\rho \sim \frac{m}{2^{r-1}(L+1)}$, which is often near 1 and at most 2.

- When $m = \frac{L+1}{2}$, we have $\rho \sim \frac{L+1}{L-1}$.
- When $\lceil \frac{2^{r+1}L}{3} \rceil \leq m \leq 2^r(L-1)-1$, the ratio can be as small as $\rho \sim \frac{4L}{3(L-1)}$ and at most $\rho \sim 2 - \frac{2}{2^r(L-1)}$.

This suggests potential for secure and efficient implementation.

Table of Family of Curves

k	L	r	m	a_1	a_2	ρ
8	37	2	111	-1	$2^{111}+2^{74}$	3/2
8	89	2	267	-1	$2^{267}+2^{178}$	3/2
8	149	2	447	-1	$2^{447}+2^{298}$	3/2
13	13	3	80	-1	$2^{80}+2^{56}$	5/3
16	13	3	91	-1	$2^{91}+2^{78}$	2
23	23	2	72	-1	$2^{72}+2^{52}$	5/3
23	23	2	80	-1	$2^{80}+2^{68}$	9/5
26	13	3	72	-1	$2^{72}+2^{40}$	3/2
26	13	3	88	-1	$2^{88}+2^{72}$	9/5
37	37	2	104	-1	$2^{104}+2^{60}$	7/5
37	37	2	112	-1	$2^{112}+2^{76}$	3/2
37	37	2	120	-1	$2^{120}+2^{92}$	5/3
37	37	2	128	-1	$2^{128}+2^{108}$	9/5
37	37	2	136	-1	$2^{136}+2^{124}$	2

Table for Security Comparison

k	L	r	m	a_1	a_2	$\log_2 N_{r,L}$	$k \log_2 q$	mk'
8	37	2	111	-1	$2^{111}+2^{74}$	143	888	296
8	89	2	267	-1	$2^{267}+2^{178}$	351	2136	712
8	149	2	447	-1	$2^{447}+2^{298}$	591	3576	1192
13	13	3	80	-1	$2^{80}+2^{56}$	95	1040	208
16	13	3	91	-1	$2^{91}+2^{78}$	95	1456	208
23	23	2	72	-1	$2^{72}+2^{52}$	87	1656	184
23	23	2	80	-1	$2^{80}+2^{68}$	87	1840	184
26	13	3	72	-1	$2^{72}+2^{40}$	95	1872	208
26	13	3	88	-1	$2^{88}+2^{72}$	95	2288	208
37	37	2	104	-1	$2^{104}+2^{60}$	143	3848	296
37	37	2	112	-1	$2^{112}+2^{76}$	143	4144	296
37	37	2	120	-1	$2^{120}+2^{92}$	143	4440	296
37	37	2	128	-1	$2^{128}+2^{108}$	143	4736	296
37	37	2	136	-1	$2^{136}+2^{124}$	143	5032	296

Yet to do...

- Construct the curves: efficient systematic way of determining the explicit coefficients of a curve when given the (a_1, a_2) parameters is not yet established.
  - CM-method for p-rank 1?
- Examine ordinary curves using similar techniques; construct using CM-methods?

In general: We still need constructions of non-supersingular pairing-friendly curves of genus $g \geq 2$.

Questions?