# Finding Vulnerable Curves Over Finite Fields of Characteristic 2 by Pairing Reduction

Yuhong Zhang
*LMAM,*
*School of Mathematical Sciences*
*Peking University*
*Beijing, China*
*yh.zhang@pku.edu.cn*

Meng Zhang
*LMAM,*
*School of Mathematical Sciences*
*Peking University*
*Beijing, China*
*menglucky@pku.edu.cn*

Maozhi Xu
*LMAM,*
*School of Mathematical Sciences*
*Peking University*
*Beijing, China*
*mzxu@pku.edu.cn*
*Corresponding Author*

***Abstract*—In this paper, we aim at sustaining the claim that curve-based cryptographic schemes over finite fields of characteristic 2 do not provide enough security. We present algorithms to find all the possible supersingular elliptic curves which can be embedded into a predefined finite field. We also consider the case of hyperelliptic curves with genus 2, including both supersingular and ordinary cases. As computational examples, we show even the DLP on a 3060-bit elliptic curve and the DLP on Jacobians of a 255-bit hyperelliptic curve can be solved by embedding to a 6120-bit extension field.**

***Keywords*-elliptic curves; hyperelliptic curves; embedding degree; discrete logarithm problem; FR-reduction.**

## I. Introduction

Over the last few decades there has been an increasing interest in pairing-based cryptography, numerous new protocols have been proposed based on the cryptographic pairings, including the well-known one-round three-way key exchange by Joux[10], ID based encryption by Boneh and Franklin[2], and so on.

The security of pairing-based cryptography is based on the computational difficulty of solving the discrete logarithm problem (DLP). By the pairing reduction, the DLP on curves can be transformed into an instance of DLP in the multiplicative group of a finite field $\mathbb{F}_{q^k}$. This is a strategy known as Frey-Ruck(FR) reduction[3] or Menezes-Okamoto-Vanstone(MOV) attack[17], depending on which pairing is considered. For certain special curves, the embedding field $F_{q^k}$ is small enough that the resulting instance can be solved using an index calculus algorithm. Apparently, this kind of strategy must rely on the developments of finite field discrete logarithms.

While in recent years, tremendous progress has been made on DLP over small characteristic finite fields, especially characteristic 2. In 2013, Joux designed a new algorithm with a complexity of $L(1/4+\varepsilon)$ in small characteristic[11]. In the same spirit, another heuristic algorithm is proposed that provides a quasi-polynomial complexity when $q$ is of size at most comparable with $k$[1]. Then the DLP on finite field of characteristic 2 got many new records[12], [13], [14], [7], [6]. Table I lists some examples.

Table I
RECORDS OF DLP ON FINITE FIELD OF CHARACTERISTIC 2

| Date | Completer | Finite Field | Time consumed |
|---|---|---|---|
| 2013.2.19 | Granger, et al. | $\mathbb{F}_{2^{1971}}$ | 3132 core hours |
| 2013.3.22 | Joux | $\mathbb{F}_{2^{4080}}$ | 14100 core hours |
| 2013.4.11 | Granger, et al. | $\mathbb{F}_{2^{6120}}$ | 749.5 core hours |
| 2013.5.21 | Joux | $\mathbb{F}_{2^{6168}}$ | 550 CPU hours |
| 2014.1.31 | Granger, et al. | $\mathbb{F}_{2^{9234}}$ | 400,000 core hours |

The breakthroughs on DLP bring the academic agreement that curves in small characteristic should be avoided for pairing-based cryptography. However, as far as we know, there is no major systematic analysis for records of DLP on curves over finite field of small characteristic through FR-reduction.

In this paper, we find elliptic and hyperelliptic curves over finite fields of characteristic 2 whose DLP can be solved by FR-reduction in spite of the huge size of base field. The rest of paper is organized as follows. We briefly introduce the FR-reduction in Section 2. In Section 3, we find supersingular elliptic curves over large subfield solvable and present explicit algorithms. In Section 4, we construct a family of hyperelliptic curve with embedding degree 12, including both supersingular and ordinary cases. We conclude the whole paper in Section 5.

## II. Using FR-reduction to break DLP on Curves

Let $C$ be a non-singular, irreducible curve of genus $g$ over a finite field $\mathbb{F}_q$. The Jacobian of the curve $C$ is an abelian variety $J_C$ of dimension $g$ defined over $\mathbb{F}_q$.

*Definition 1 (Tate pairing[3]):* Let $l$ be a positive integer which is coprime to $q$. In most applications $l$ is a prime and $l|\#J_C(\mathbb{F}_q)$. Let $k$ be a positive integer such that the field $\mathbb{F}_{q^k}$ contains the $l$th roots of unity (in other words, $l|(q^k-1)$). Let $G = J_C(\mathbb{F}_{q^k})$ and write $G[l]$ for the subgroup of divisors of order $l$ and $G/lG$ for the quotient group (which is also a group of exponent $l$). Then the Tate pairing is a mapping

$$\langle\cdot,\cdot\rangle : G[l]\times G/lG \longrightarrow \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^l. \tag{1}$$

Let $D_1, D_2 \in J_C(\mathbb{F}_q)$ be divisors of order $l$ for which we want to solve the discrete logarithm problem $D_2 = \lambda D_1$.

978-1-5090-5507-4/17/$31.00 ©2017 IEEE
ICIS 2017, May 24-26, 2017, Wuhan, China

Let $k$ be the smallest integer such that $l|(q^k-1)$. The FR-reduction proceeds as follows:

1) Choose random divisors $Q \in J_C(\mathbb{F}_{q^k})$ until $< D_1, Q > \notin (\mathbb{F}^*_{q^k})^l$ .
2) Computer $\xi_i =< D_i, Q > \in \mathbb{F}^*_{q^k}$.
3) Map the $\xi_i$ to $l$th roots of unity (by raising to the power $(q^k-1)/l$). This step is actually optional since the linear algebra in the index calculus method should be performed modulo $l$.
4) Solve the discrete logarithm problem $\xi_2 = \xi_1^\lambda$ in the subgroup of order $l$ of the finite field $\mathbb{F}^*_{q^k}$ using an index calculus method.

This strategy is practical when $k$ is small. We note in FR-reduction, DLP on Jacobians $J$ is reduced to DLP for the smallest integer $k$ such that $l|(q^k-1)$. In other words, $k$ is minimal such that $l|\phi_k(q)$ where $\phi_k(x)$ is the $k$th cyclotomic polynomial. $k$ is usually called embedding degree.

## III. Finding vulnerable elliptic curves over finite fields $\mathbb{F}_{2^m}$

In Table I, we show currently the ability of solving DLP on $\mathbb{F}_{2^n}$ is far in front of the other cases, thus it is possible to find elliptic curves over large subfield $\mathbb{F}_{2^m}$ solvable through FR-reduction.

To our knowledge, in the case of finite field of characteristic 2, there is little information available about ordinary elliptic curves with small embedding degree, thus supersingular elliptic curves become the only choice for pairing-based cryptography.

Therefore, we focus on supersingular elliptic curves in this section.

*Definition 2 (supersingular elliptic curve):* Let $q = p^s$ for some prime $p$ and $s \in N$. An elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q+1-t$ is supersingular if and only if $gcd(t,q) > 1$.

Waterhouse [18] showed that supersingular curves all have small embedding degree $k \in \{1,2,3,4,6\}$. For fields of characteristic 2 and 3, representatives for each $\mathbb{F}_q$-isomorphism class of supersingular curves have been determined by Menezes and Vanstone [16]. In this paper, we only consider the finite fields of characteristic 2, the supersingular elliptic curves on which only has embedding degrees $k \in \{1,2,3,4\}$. The Table II lists all possibilities for embedding degree and number of points for supersingular elliptic curves over finite field $\mathbb{F}_{2^m}$.

Table II
NUMBER OF POINTS FOR SUPERSINGULAR ELLIPTIC CURVES OVER $\mathbb{F}_{2^m}$

| k | q | $\#E(\mathbb{F}_q)$ |
|---|---|---|
| 1 | $2^{2a}$ | $q \pm 2\sqrt{q}+1$ |
| 2 | $2^{2a+1}$ | $q+1$ |
| 2 | $2^{2a}$ | $q+1$ |
| 3 | $2^{2a}$ | $q \pm \sqrt{q}+1$ |
| 4 | $2^{2a+1}$ | $q \pm \sqrt{2q}+1$ |

### A. An algorithm to find vulnerable elliptic curves

When a finite field $\mathbb{F}_{2^n}$ is given, we hope to find all the possible supersingular elliptic curves defining on $\mathbb{F}_{2^m}$ which can be embedded into $\mathbb{F}_{2^n}$ by FR-reduction. Apparently $m|n$ is satisfied.

Before describing the algorithm, we give some explanations on the parameter:

1) When $k=1$, then $n$ must be even. Taking $m=2m'$ satisfying $m'|n/2$, then $l=2^{m'}+1$ or $l=2^{m'}-1$.
2) When $k=2$, taking $m=m'$ satisfying $m'|n$, then $l=2^{m'}+1$.
3) When $k=3$, then $6|n$. Taking $m=2m'$ satisfying $m'|n/6$, then $l=2^{2m'}+2^{m'}+1$ or $l=2^{2m'}-2^{m'}+1$.
4) When $k=4$, then $4|n$. Taking $m=2m'+1$ satisfying $(2m'+1)|n/4$, then $l=2^{2m'+1}+2^{m'+1}+1$ or $l=2^{2m'+1}-2^{m'+1}+1$.

Following the notation above, we present Algorithm 1.

**Algorithm 1** Finding supersingular elliptic curves with embedding degree $k$.

**Input:** $k$, $2^n$.
**Output:** the supersingular elliptic curves over $\mathbb{F}_{2^m}$ with embedding degree $k$ which can be embedded into $\mathbb{F}_{2^n}$.

1: **for** all the possible $l$ **do**
2: factor $l$,
3: **while** a prime factor $N|l$ satisfying $\sqrt{2^m} < N < 2^m+1+2\sqrt{2^m}$ **do**
4: A suitable $E/\mathbb{F}_{2^m}$ is obtained, which has $l$ points and a large subgroup with $N$ points,
5: Get curve equation by the classification of isomorphism class of supersingular curves[16].
6: **end while**
7: **end for**

### B. Examples

*1) Finding elliptic curves which can be embedded into $\mathbb{F}_{2^{6168}}$:*

We have known in Table I that the DLP on $\mathbb{F}_{2^{6168}}$ has been solved with 550CPU-hours in 2013. We now fix the finite field as $\mathbb{F}_{2^{6168}}$, then use algorithm 1 to find the supersingular elliptic curves which can be embedded into it by FR-reduction.

n=6168=8*3*257, so the possible $k$ can be chosen from $\{1, 2, 3, 4\}$.

- $k = 3$:
  Computer $l = 2^{514} + 2^{257} + 1$, we find a large prime number $N$ of 501-bit satisfying $N|l$ where
  $N = 4965395030068548134274243124972075225434447114375481299036593442726326832727934403424309955102162841656341524725641213163998408700663382552888660520657$.
  We get the elliptic curve as follows:
  $$E/\mathbb{F}_{2^{257*2}} : y^2 + ay = x^3 + a^{513},$$
  in which $a$ is the generator of $F_{2^{257*2}}$. It can be seen that $\#E(\mathbb{F}_{2^{257*2}}) = 2^{514} + 2^{257} + 1$ and $E$ has a subgroup with $N$ points.
- $k = 4$:
  1) Computer $l = 2^{257} + 2^{129} + 1$, we find a large prime number $N$ of 202-bit satisfying $N|l$ where
  $N = 4501721456014165137144897707223043167472851489652285029320729$.
  We get the elliptic curve as follows:
  $$E/\mathbb{F}_{2^{257}} : y^2 + y = x^3 + x,$$
  It satisfies that $\#E(\mathbb{F}_{2^{257}}) = 2^{257} + 2^{129} + 1$ and has a subgroup with N points.
  2) Computer $l = 2^{257} - 2^{129} + 1$, we find a large prime number $N$ of 223-bit satisfying $N|l$. We get the elliptic curve as follows:
  $$E/\mathbb{F}_{2^{257}} : y^2 + y = x^3 + x + 1.$$
  It can be seen that $\#E(\mathbb{F}_{2^{257}}) = 2^{257} - 2^{129} + 1$ and E has a subgroup with N points.

*2) Finding elliptic curves which can be embedded into $\mathbb{F}_{2^{6120}}$:*

The DLP on $\mathbb{F}_{2^{6120}}$ has been solved with 749.5 core-hours in 2013. We now fix the finite field as $\mathbb{F}_{2^{6120}}$, then find suitable supersingular elliptic curves.

$n = 6120 = 8 * 9 * 85$, so the possible $k$ can be chosen from $\{1, 2, 3, 4\}$.

- $k = 2$:
  Computer $l = 2^{3060} + 1$, we find a large prime number $N$ of 1536-bit satisfying $N|l$ where
  $N = 2409724115404494827286220495589956719490433386718129246307340879766614099596764069319462057403289158066872442577677895069481188262037263465851544618816793500449547854226438488296334629850630746872267441710129445332438813133451158969357109043507671389433684761619990070069339844732442243277967167350323374086576244912070758401182983154676250566511391799888801677787864202019144725684891765622386647326057292307527811142296983316685543634953548660537734789823305728 1.

We get the elliptic curve as follows:

$$E/\mathbb{F}_{2^{3060}} : y^2 + y = x^3 + a^{3047}x,$$

in which $a$ is the generator of $\mathbb{F}_{2^{3060}}$. It can be seen that $\#E(\mathbb{F}_{2^{3060}}) = 2^{3060} + 1$ and $E$ has a subgroup with $N$ points.

- $k = 3$: Computer $l = 2^{2040} + 1$, we find the same large prime number $N$ of 1536-bit satisfying $N|l$. We get the elliptic curve as follows:
  $$E/\mathbb{F}_{2^{2040}} : y^2 + ay = x^3 + a^{2035}x,$$
  in which $a$ is the generator of $\mathbb{F}_{2^{2040}}$. It can be seen that $\#E(\mathbb{F}_{2^{2040}}) = 2^{2040} - 2^{1020} + 1$ and $E$ has a subgroup with $N$ points.

## IV. Finding vulnerable hyperelliptic curves of Genus 2 over finite fields $\mathbb{F}_{2^m}$

In this section, we find hyperelliptic curves over large subfield $\mathbb{F}_{2^m}$ solvable through FR-reduction.

### A. Hyperelliptic curves

A hyperelliptic curve $C$ of genus $g$ is a curve with an equation of the form

$$y^2 + h(x)y = f(x)$$

where $h(x)$ and $f(x)$ are polynomials with $deg(f) = 2g + 1$ or $2g + 2$ and $deg(h) \leq g$, the Jacobian group of $C$ is noted as $J_C(\mathbb{F}_q)$. The bound of point number of hyperelliptic curves is given in Lemma 1, which is a generalization of the case of elliptic curves.

*Lemma 1:* Let $C$ be a hyperelliptic curve of genus $g$ defined over a finite field $F_q$. Then we have

$$(\sqrt{q} - 1)^{2g} \leq \#J_C(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}. \quad (2)$$

Let $\chi(t)$ be the characteristic polynomial of the $q$th power Frobenius endomorphism of $C$. We call $\chi(t)$ for $C$ the characteristic polynomial of $C$, which is of the form

$$\chi(t) = t^{2g} + a_1 t^{2g-1} + \ldots + a_g t^g + q a_{g-1} t^{g-1} + \ldots + q^{g-1} a_1 t + q^g. \quad (3)$$

There is a relationship with the $\chi(t)$ and $\#J_C(\mathbb{F}_q)$.

*Lemma 2:* The order of $J_C(\mathbb{F}_q)$ is given by

$$\#J_C(\mathbb{F}_q) = \chi(1). \quad (4)$$

### B. Construction

The main observation that leads to the construction is the special case $k = 12$ in the paper [4].

*Lemma 3:* Let $\phi_{12}$ be the 12th cyclotomic polynomial. Then $\phi_{12}(2l^2) = n(l)n(-l)$ where $n(l) = 4l^4 + 4l^3 + 2l^2 + 2l + 1$.

According to Lemma 3, we take $l = 2^m$ and get $q = 2l^2 = 2^{2m+1}$, then the curve $C$ over $F_q$ with $n(l)$ or $n(-l)$ points has embedding degree $k = 12$.

1) If curve $C$ has $n(l)$ points, then

$$n(l) = 4l^4 + 4l^3 + 2l^2 + 2l + 1 = q^2 + \sqrt{2q}(q+1) + q + 1. \quad (5)$$

Notice

$$(\sqrt{q} - 1)^{2*2} \leq n(l) \leq (\sqrt{q} + 1)^{2*2}. \quad (6)$$

so the only possible case is hyperelliptic curves of genus 2. Writing the characteristic polynomial as

$$\chi(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2. \quad (7)$$

we have

$$\chi(1) = q^2 + a_1(q+1) + a_2 + 1 = n(l). \quad (8)$$

We can give two sets of parameters:

i) $a_1 = \sqrt{2q}$ and $a_2 = q$
ii) $a_1 = \sqrt{2q} + 1$ and $a_2 = q + 1$

2) If curve $C$ has $n(-l)$ points, then

$$n(-l) = 4l^4 - 4l^3 + 2l^2 - 2l + 1 = q^2 - \sqrt{2q}(q+1) + q + 1. \quad (9)$$

Notice

$$(\sqrt{q} - 1)^{2*2} \leq n(-l) \leq (\sqrt{q} + 1)^{2*2}. \quad (10)$$

so the only possible case is hyperelliptic curves of genus 2. Writing the characteristic polynomial as

$$\chi(t) = t^4 + a_1 t^3 + a_2 t^2 + q a_1 t + q^2. \quad (11)$$

we have

$$\chi(1) = q^2 + a_1(q+1) + a_2 + 1 = n(-l). \quad (12)$$

We can give two sets of parameters:

i) $a_1 = -\sqrt{2q}$ and $a_2 = q$
ii) $a_1 = -\sqrt{2q} + 1$ and $a_2 = q + 1$

Theorem 1 offers a criteria to check whether a curve $C$ is supersingular or not.

*Theorem 1 ([5]):* Suppose $q = p^n$ and suppose $C$ is a hyperelliptic curve of genus $g$ over $\mathbb{F}_q$. Suppose

$$\chi(t) = t^{2g} + a_1 t^{2g-1} + \ldots + a_g t^g + q a_{g-1} t^{g-1} + \ldots + q^{g-1} a_1 t + q^g, \quad (13)$$

is the characteristic polynomial of the Frobenius endomorphism on $C$. Then $C$ is supersingular if and only if for all $1 \leq r \leq g$, $p^{\lceil rn/2 \rceil} | a^r$.

By Theorem 1, we see the curve with $a_1 = \pm\sqrt{2q}$ and $a_2 = q$ is supersingular, while the curve with $a_1 = \pm\sqrt{2q} + 1$ and $a_2 = q + 1$ is ordinary.

For convenience, we give the equations of supersingular case, which has been thoroughly studied by Koblitz[8], [9]:

The equation of curve with $a_1 = \pm\sqrt{2q}$ and $a_2 = q$ are given by

$$y^2 + y = x^5 + x^3,$$

or

$$y^2 + y = x^5 + x^3 + 1.$$

### C. An example

*1) Finding hyperelliptic curves which can be embedded into $\mathbb{F}_{2^{6120}}$:*

Similar to Section III-B, we fix the finite field as $\mathbb{F}_{2^{6120}}$, then find hyperelliptic curve $C$ of genus 2 which can be embedded into it by FR-reduction.

We choose the base field as $\mathbb{F}_q = \mathbb{F}_{2^{255}}$ and computer $l = 2^{127}$.

Let the point number of $C$ be $n(-l) = 4l^4 - 4l^3 + 2l^2 - 2l + 1$ where $n(-l)$ is a 510-bit number. We find a large prime number $N$ of 323-bit satisfying $N | n(-l)$ where
$N = 27114441376001634978955573621759309290499573081114532534505305002578255791764403844101991735185701.$

As a result, we obtain the hyperelliptic curve $C$ with embedding degree 12 as follows:

$$C/\mathbb{F}_{2^{255}} : y^2 + y = x^5 + x^3 + 1.$$

It can be seen that $\#J_C(\mathbb{F}_{2^{255}}) = n(-2^{127})$ and $C$ has a subgroup with $N$ points.

## V. Conclusion

In this paper, we give the records of DLP on curves over finite field of characteristic 2 through FR-reduction. Our work shows that curves over finite fields of characteristic 2 cannot provide enough security even if the size of finite field reached 3060 bits, which would serve as a confirmation that finite fields of characteristic 2 should be definitely avoided for pairing-based cryptography.

## References


[1] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé, "A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic," In Advances in Cryptology-EUROCRYPT 2014, volume 8441 of LNCS, pages 1-16. Springer, 2014.

[2] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, 2003, 32(3):213-229.

[3] G. Frey and H. G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," Mathematics of computation, 62(1994), 865-874.

[4] S. Galbraith, J. McKee and P. Valença, "Ordinary abelian varieties having small embedding degree," Finite Fields Appl. 13, 800-814 (2007).

[5] S. D. Galbraith, "Supersingular curves in cryptography," In Advances in Cryptology-ASIACRYPT 2001 (Gold Coast), volume 2248 of Lecture Notes in Computer Science, pages 495-513. Springer-Verlag, Berlin, 2001.

[6] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, "Solving a 6120-bit DLP on a desktop computer," In Selected Areas in Cryptography-SAC 2013, volume 8282 of LNCS, pages 136-152. Springer, 2014.

[7] R. Granger, T. Kleinjung, and J. Zumbrägel, "Discrete Logarithms in $GF(2^{9234})$," NMBRTHRY list, 31/1/2014.

[8] N. Koblitz, "Hyperelliptic cryptosystems," J. Cryptology, 1, no. 3 (1989) 139-150.

[9] N. Koblitz, "A family of jacobians suitable for discrete log cryptosystems," in S. Goldwasser (ed.), Crypto'88, Springer LNCS 403 (1990) 94-99.

[10] A. Joux, "A one round protocol for tripartite Diffie-Hellman," Journal of Cryptology, 17(4):385-393 (2006)

[11] A. Joux, "A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic," In Tanja Lange, Kristin Lauter, and Petr Lisoněk, editors, Selected Areas in Cryptography-SAC 2013, volume 8282 of LNCS, pages 355-379. Springer, 2014.

[12] A. Joux, "Discrete logarithm in $GF(2^{1778})$ (Feb 2013)," announcement to the NM-BRTHRY list.

[13] A. Joux, "Discrete logarithm in $GF(2^{4080})$ (Mar 2013)," announcement to the NM-BRTHRY list.

[14] A. Joux, "Discrete logarithm in $GF(2^{6168})$ (May 2013)," announcement to the NM-BRTHRY list.

[15] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," IEICE Trans. Fundam. E84-A(5), 1234-1243 (2001).

[16] A. Menezes and S. Vanstone, "Isomorphism classes of elliptic curves over finite fields of characteristic 2," Util. Math. 38, 135-153 (1990).

[17] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," IEEE Trans. Inform. Theory. 39(5), 1639-1646 (1993).

[18] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields," Ann. Sci. École Norm. Sup. (IV) 2, 521-560 (1969).