Elliptic Curves : The state of the art

Matthijs Coster

12 april 2002

Contents

1 Introduction

At the Elliptic Curve Conference 2002 in Waterloo (Canada) many researchers on elliptic curve cryptography were explaining their ideas on (hyper)elliptic curves. Given these talks I think in elliptic–curves–cryptography the research is still going faster than any of the other areas of public key cryptography. This presentation, I will go into detail in some of the subjects on which the research is pointed.

1. Counting points
2. Hyperelliptic Curves
3. Attacks on Elliptic Curves

2 Counting points

There are several ways to count points. We mention:

1. checking point after point
2. Baby–step Giant–step
3. SEA (Schoof, Elkies, Atkin)
4. Satoh–FGH (Fouquet, Gaudry, Harley) (only $\mathbb{F}_{p^n}$, p small)
5. AGM (Mestre, Gaudry, Harley) (only $\mathbb{F}_{2^n}$)

We distinguish the finite fields $\mathbb{F}_p$, $\mathbb{F}_{p^n}$, where $p > 2$ but p small and $\mathbb{F}_{2^n}$. We have the following table with records upto now:

records for counting points on elliptic curves			
Field $\mathbb{F}_q$	researcher(s)	year	CPU–time
$10^{499} + 153$	R. Lercier and F. Morain	1995	$\frac{1}{2}$ year
5^{569}	Satoh	1999	1 month
2^{16001}	R. Harley	2001	1 month

It is remarkeble how large the size of the largest $\mathbb{F}_{2^n}$-field is on which the points of an elliptic curve are counted. For curves on $\mathbb{F}_p$ only the SEA–algorithm

(Schoof, Elkies, Atkin) can be applied, however on the field $\mathbb{F}_{p^n}$ we can choose for SEA and Satoh. Satoh's method is based on the *Verschiebung*, a map which goes in the opposite direction as the Frobenius Endomorphism. Most recently Fouquet, Gaudry and Harley published an improved method based on the Verschiebung. Their new algorithm is called Algebraic–Geometric–Mean, and it works in the same way as the method to calculate π very accurate.

Harley and his company ArgoTech implied the algorithm for finding an Elliptic Curve with a number of points, which contain only one large prime divisor. The speed of the algorithm is comparable to creating an RSA–key.

Time to find "good" elliptic curves		
# bits	time	RSA–equivalent (bits–length)
163	2 sec.	1416
197	5 sec.	2054
239	8 sec.	3061

3 Hyperelliptic Curves

There can be said a lot about hyperelliptic curves. Unfortunately the time to do that is very restricted. Therefore this has to be done another time. I restrict myself to a definition and some remarks on the attacks on hyperelliptic curves. The main reason to tell something about hyperelliptic curves is the fact that the newest attacks on elliptic curves can be reduced to attacks on hyperelliptic curves.

An *hyperelliptic curve* $\mathcal{H}_q$ over $\mathbb{F}_q$ is defined by:

$$\mathcal{H}_q : y^2 + f(x)y = h(x),$$

with $f(x), h(x) \in \mathbb{F}_q[x]$, $\deg(f(x)) < \deg(h(x))$. The *genus* g of $\mathcal{H}_q$ is defined by $g = \left\lfloor \frac{\deg(h)-1}{2} \right\rfloor$. If $g = 1$ then the curve is elliptic as well. The set of points on $\mathcal{H}_q$ is defined by $\mathcal{H}_q = \{(x, y) : x, y \in \mathbb{F}_q, y^2 + f(x)y = h(x)\} \bigcup \mathcal{O}$, here $\mathcal{O}$ is the point at infinity. If it is clear which group is used, we often denote $\mathcal{H}$ instead of $\mathcal{H}_q$.

Unfortunately the points on $\mathcal{H}$ do not form a group. However we can consider $\mathbb{J}$, the *Jacobian*. In order to define the Jacobian we consider *divisors*, abstract sums of points: $\sum_i n_i P_i$. The set of divisors $\mathcal{D}$ forms a group. Especially, we consider two subgroups of $\mathcal{D}$. $\mathcal{D}^0$ is the subgroup of divisors of degree 0 (i.e. $\sum_i n_i = 0$). The subgroup $\mathcal{P} \subset \mathcal{D}^0$ is formed by the set of divisors which can be defined by functions $k(x, y) \in \mathbb{F}_q(x, y)/(y^2 + f(x)y - h(x))$ (the *principal divisors*). The more detailed definition is more complicated, and will be postponed to another Cryptography Workinggroup Day (maybe?), however, the interested reader can find a reference in [20]. To get the Jacobian we consider the quotientgroup $\mathbb{J} = \mathfrak{D}^0/\mathfrak{P}$. The number of elements of the Jacobian is bounded by the theorem of Weil, which tells that:

$$(\sqrt{q} - 1)^{2g} \leq \#\mathbb{J} \leq (\sqrt{q} + 1)^{2g} .$$

3.1 Counting points on hyperelliptic curves

It is much harder to count the points on hyperelliptic curves than on elliptic curves. New methods are topic of research at the moment. Gaudry (cf. [1]) told about what he expected what will be found.

counting points on (hyper)elliptic curves			
	$g = 1$ (Elliptic Curves)	$g = 2$	$g = 3$
$p = 2$	SEA & Satoh/FGH/Kedlaya	Satoh	
p small	SEA & Satoh/Kedlaya	Kedlaya/GG	Kedlaya/GG
p large	SEA		

Kedlaya published another method (cf. [17]). This method will be one of the topics of ECC2002 (cf. [2]).

records for counting points on hyperelliptic curves ($g = 2$)			
Field $\mathbb{F}_q$	researcher(s)	year	CPU–time
$10^{19} + 51$	P. Gaudry & R. Harley	2000	1 year
3^{30}	P. Gaudry & R. Harley	2000	short

3.2 Attacks on hyperelliptic curves

In general there are several ways to attack a discrete logarithm. We list them below:

1. Exhausted search
2. Baby–step Giant–step

3. Pollard's rho

4. Pohlig–Hellman

5. Index calculus

Most of them are well known. The last attack needs some explanation. In the case of the usual Discrete Logarithm the Index calculus can be applied. We start with a *factor base* $\mathfrak{F} = \{p_1, \ldots, p_k\}$. For several exponents x_j we try to factor g^{x_j} in factors which are contained in $\mathfrak{F}$. If the number of equations is larger than the number of elements in the factorbase, then the elements of the factorbase can be expressed as a power of g. With this knowledge it is easier to express arbitrary elements h and h' as powers of g. Therefore a subexponential attack is possible. The attack described here has an expected running time of $L_q(\frac{1}{2}, \lambda_1)$, however the algorithm based on NFS has even an expected running time of $L_q(\frac{1}{3}, \lambda_2)$.

In the case of hyperelliptic curves (of genus ≥ 2) it is possible as well to describe a factor basis (starting with the points on the curve). A subexponential attack with running time $L_q(\frac{1}{2}, \lambda_3)$ was found by Adleman, DeMarrais and Huang (cf. [4]), and later improved by Gaudry and Enge (cf. [9] & [8]). At the moment the index calculus attack is faster than Pollard's rho except for the genera $g = 2$ and $g = 3$.

record attacks on (hyper)elliptic curves				
	DL	$g = 1$ (Elliptic Curves)	$g = 2$	$g = 3$
$p = 2$	$\mathbb{F}_{2^{607}}$	$\mathbb{F}_{2^{108}}$	???	???
p large	???	97 bits–prime	???	???

In [9] Gaudry describes two attacks for large genera:

results of Gaudry			
Field	curve	#points	time
$\mathbb{F}_p, p = 5026243$	$y^2 + y = x^{13}$	10^{41}	15 days
$\mathbb{F}_{2^{23}}$	$y^2 + (x+1)y = x^{13} + \ldots + 1$	10^41	21 days

3.3 New research on hyperelliptic curves

An enormous amount of work is spend on research on the HCDL. During the last ECC Weng (cf. [1]) showed that using hyperelliptic curves with complex multiplication it is feasable to calculate the size of the Jacobian. She was even able to make a program to select "good" hyperelliptic curves for HCDL. She didn't answer the question *how safe are those curves?*.

4 Attacks on Elliptic Curves

The list of attacks on the ECDLP is about the same as for hyperelliptic curves.

1. Exhausted search
2. Baby–step Giant–step
3. Pollard's rho
4. Pohlig–Hellman
5. Index calculus
6. Special Curves

Upto now nobody was able to find a good factor base in order to apply the Index calculus. In 1998 Silverman suggested a way to apply the Index calculus (cf. [22]). His attack failed (cf. [15]). The list of special curves becomes longer and longer:

- supersingular curves (trace 0 curves over $\mathbb{F}_p$), *Menezes, Okamoto, Vanstone*
- anomalous curves (trace 1 curves over $\mathbb{F}_p$), *Frey, Rück, Semaev, Satoh, Araki, Smart*
- trace 2 curves over $\mathbb{F}_p$ (based on the Tate–pairing), *Frey, Müller, Rück*
- recent research using the Weil descent over $\mathbb{F}_{2^n}$, *Frey, Gaudry, Hess, Smart, Galbraith, Jacobson, Menezes, Stein, Maurer, Teske*

4.1 An attack based on the Weil descent

Most recent research of Gaudry, Hess, Smart, Galbraith, Jacobson, Menezes, Stein, Maurer, Teske is based on the work of Frey (ECC, 1998). The basic idea is to replace the Elliptic Curve $\mathcal{E}$ over $\mathbb{F}_{q^m}$ by an m-dimensional abelian variety $\mathcal{W}$ over $\mathbb{F}_q$ (here $q = p^l$, in general $p = 2$). Sometimes it is possible to intersect the abelian variety by $m-1$ hyperplanes, in such a way that the intersection is a hyperelliptic curve. Now we are able to reduce the ECDLP over $\mathbb{F}_{q^m}$ to an HCDLP over $\mathbb{F}_q$, which can be solved easily, because there exists a factor base for hyperelliptic curves.

Let $K = \mathbb{F}_{2^n}$, and let the elliptic curve

$$\mathcal{E} : Y^2 + XY = X^3 + AX^2 + B$$

be defined over K, i.e. $A, B \in K$. Suppose $n = lm$. Let $q = 2^l$, $k = \mathbb{F}_q$, then K is an extension of k of degree m. Hence there exists a k–basis $\psi_0, \psi_1, \ldots, \psi_{m-1}$. We can express A, B, X, Y in terms of the elements of the k–basis:

$$\begin{aligned}
A &= a_0\psi_0 + a_1\psi_1 + \ldots a_{m-1}\psi_{m-1} \\
B &= b_0\psi_0 + b_1\psi_1 + \ldots b_{m-1}\psi_{m-1} \\
X &= x_0\psi_0 + x_1\psi_1 + \ldots x_{m-1}\psi_{m-1} \\
Y &= y_0\psi_0 + y_1\psi_1 + \ldots y_{m-1}\psi_{m-1}
\end{aligned}$$

After substituting these equations in the equation of the elliptic curve, we get an equation of a variety $\mathcal{W}$ over k in $2m$ variables. $\mathcal{W}$ is called the *Weil restriction*, and the process is called the *Weil descent*.

The next step is to find a hyperelliptic curve $\mathcal{H}_q$ as a sub–variety in $\mathcal{W}$, with the property:

$$\#\mathbb{J}(\mathcal{H}_q) = \#\mathcal{E}_{q^m}.$$

This is rather complicated. The interested reader is invited to read [13], [12], [19], [14] to learn more about this step. Often this step will fail.

The idea was mentioned by Frey at ECC1998 (cf. [1]). The first complete paper [12] was written by Gaudry, Hess, Smart. They are still very negative about getting results:

We wish to find a curve $\mathcal{H}$ in $\mathcal{W}$ whose Jacobian contains a subvariety isogenous to $\mathcal{V} \subset \mathcal{W}$.

and

..., but it is highly unlikely such a curve [$\mathcal{H}$] exists at all.

Later Jacobson, Menezes, Stein found an approach [16] to apply the GMS–attack. their idea was: Suppose for $\mathcal{E}_1$ GHS cannot be applied, try to find an isogenous curve $\mathcal{E}_2$. The Weil descent of $\mathcal{E}_2$ differs from the Weil descent of $\mathcal{E}_1$. Repeat this step until you are lucky.

Hess wrote a KASH–program implementing the ideas of JMS.

Maurer, Menezes and Teske applied this KASH–program on several cases in the real cryptographical world. I cite from their paper [18]

It was proven to fail for all *cryptographycally interesting elliptic curves over $\mathbb{F}_{2^n}$, where $n \in [160, 600]$ is prime.*

The purpose of this paper is to investigate the applicability of the GHS attack on the ECDLP for cryptographycally interesting elliptic curves over $\mathbb{F}_{2^n}$ for composite $n \in [160, 600]$.

and

... Hess's KASH implementation of the algorithm [of the Weil descent] takes atmost a few hours on a workstation.

In their paper they have a table for values n between 100 and 600. I select the values between 160 and 170.

Examples of Maurer, Menezes & Teske					
Field $\mathbb{F}_{2^n}$	m	l	GHS	ρ	improvement
160	20	8	52	79	27
161	7	23	34	80	46
162	54	3	42	80	38
163	—	—	—	81	—
164	4	41	45	81	36
165	15	11	37	82	45
166	2	83	83	82	—
167	—	—	—	83	—
168	7	24	35	83	48
169	13	13	1208	84	—

In the table m and l are the same as mentioned before: $n = ml$. In the column HCDLP the 2–log of the running times are written for the GHS attack. In the column ρ the running times are written for Pollard–ρ, in the last column the differences are written.

Remark In [5] Arita shows that the Weil descent can be used as well for other small primes. Diem shows in [6] that a GHS–like attack can be used for those small primes.

5 ECC 2002

This year the Elliptic Curve Cryptography Conference will be organised in Essen (Germany). The organisation recently announced that the following speakers confirmed a submission:

- Dan Bleichenbacher (Lucent Technologies, USA)
- Steven Galbraith (Royal Holloway College, UK)
- Kiran Kedlaya (University of California, Berkeley, USA)
- Alan Lauder (Oxford University, UK)
- Kumar Murty (University of Toronto, Canada)
- Phong Nguyen (ENS, Paris, France)
- David Pointcheval (ENS, Paris, France)
- Takakazu Satoh (Saitama University, Japan)
- René Schoof (University of Rome, Italy)
- Frederik Vercauteren (Katholieke Universiteit Leuven, Belgium)

6 Literature

References

[1] **Alfred Menezes, Edlyn Teske**, *ECC2001 Conference*, http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/.

[2] **Gerhard Frey, Annegret Weng**, *ECC2002 Conference*, http://www.exp-math.uni-essen.de/ weng/ecc2002.html.

[3] **Matthijs Coster**, *Elliptische Krommen : Een overzicht*, http://www.coster.demon.nl/elliptic/index.html.

[4] **Leonard M. Adleman, Jonathan DeMarrais, Ming-Deh Huang**, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields* pp. 28–40, ANTS–I , LNCS 877, Springer–Verlag, Berlin (1994).

[5] **Seiko Arita**, *Weil descent of elliptic curves over finite fields of characteristic three* pp. 248–258, Asiacrypt 2000, LNCS 1976, Springer–Verlag, Berlin (2000).

[6] **Claus Diem**, *The GHS–attack in odd characteristic*, (2002), to appear.

[7] **Andreas Enge**, *Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time*, (1999), to appear.

[8] **Andreas Enge, Pierrick Gaudry**, *A General Framework for Subexponential Discrete Logarithm Algorithms*, (2000), to appear, Rapport de Recherche Lix/RR/00/04, June 2000. Available from http://ultralix/polytechnique.fr/Labo/Pierrick.Gaudry/papers.html.

[9] **Pierrick Gaudry**, *An algorithm for solving the discrete log problem on hyperelliptic curves*, pp. 19–34, Advances in Cryptology, Eurocrypt 2000, Springer–Verlag, LNCS 1807, (2000).

[10] **Pierrick Gaudry, Nicolas Gürel**, *An extension of Kedlaya's algorithm to superelliptic curves*, pp. 480–494, Advances in Cryptology, Asiacrypt 2001, Springer–Verlag, LNCS 2248, (2001).

[11] **Pierrick Gaudry, Robert Harley**, *Counting Points on Hyperelliptic Curves over Finite Fields*, (2000), to appear.

[12] **Pierrick Gaudry, Florian Hess, Nigel P. Smart**, *Constructive and destructive facets of Weil descent on elliptic curves*, (2002), to appear in Journal of Cryptology.

[13] **Steven D. Galbraith, Nigel P. Smart**, *A cryptographic application of Weil Descent*, pp. 191–200, IMA – Cryptography & Coding 1999, Springer–Verlag, LNCS 1746, (1999).

[14] **Florian Hess**, *Extending the GHS Weil descent attack*, (2002), to appear in Eurocrypt 2002.

[15] **Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, Edlyn Teske**, *Analysis of the Xedni Calculus Attack*, Designs, Codes & Cryptography, (2000).

[16] **Michael J. Jacobson, Alfred Menezes, Andreas Stein**, *Solving elliptic curve discrete logarithm problems using Weil descent*, (2001), to appear.

[17] **Kiran S. Kedlaya**, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, (2001), to appear. Preprint available at http://arXiv.org/abs/math/0105031

[18] **Markus Maurer, Alfred J. Menezes, Edlyn Teske**, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree*, (2001), to appear.

[19] **Alfred J. Menezes, Minghua Qu**, *Analysis of the Weil descent attack of Gaudry, Hess and Smart*, (2001), to appear.

[20] **Alfred J. Menezes, Yi–Hong Wu, Robert J. Zuccherato**, *An elementary introduction to hyperelliptic curves*, Algebraic Aspects of Cryptography, (Neal Koblitz), ACM 3, Springer–Verlag, Berlin (1996).

[21] **Takakazu Satoh**, *The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting*, (1998), to appear.

[22] **Joseph H. Silverman**, *The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem*, Designs, Codes & Cryptography, (2000).

[23] **Berit Skjernaa**, *Satoh point counting in characteristic 2*, (2000), to appear.