Arcana-ECDB - A database of elliptic curves - Version 2.0

1 Introduction, notations

Arcana-ECDB is a part of the **Arcana Project** from the **eRISCS** team of Aix-Marseille University and the expert group of the **ACrypTA association**. It provides a database of elliptic curves suitable for cryptography.

The database is splitted in three parts : "Edwards", "Montgomery", "Weierstrass" which contains respectively elliptic curves given by an Edwards equation, a Montgomery equation, a short Weierstrass equation. Each part contains five sections : curves of size about 160 bits, 256 bits, 384 bits, 512 bits. In each section, we have defined 18 curves. Each curve is defined by a file (for example e256-003.gp, w512-012.gp, e384-005.gp).

Then the repository has the following folders structure :

- elliptic_curves
  - Edwards
    - ce160, ce192, ce256, ce384, ce512
  - Montgomery
    - cm160, cm192, cm256, cm384, cm512
  - Weierstrass
    - cw160, cw192, cw256, cw384, cw512

2 Elliptic curves in short Weierstrass form

We are looking for curves

$$y^2 = x^3 + a4 * x + a6$$

over a finite prime field $\mathbb{F}_p$ where the size of p is about 256 bits, 384 bits, 512 bits. Moreover $p \equiv 3 \mod 4$. This simplifies the computation of the square roots in $\mathbb{F}_p$. Let n be the number of $\mathbb{F}_p$-rational points of the curve. The Weierstrass curves given in the database are such that n is prime. The curves are drawn at random. To prove that the curves are not particular, we draw two random numbers $r1$ and $r2$ and we take for $a4$ and $a6$ the hash values of $r1$ and $r2$. A point $g = (gx, gy)$ of the curve is also given. The x-coordinate gx is the hash value of a random r and is such that $x^3 + ax + b$ is a square.

Then the file descriptor of such a curve contains 9 lines defining the parameters p,n,$a4$,$a6$,$r4$,$r6$,gx,gy,r.

p	$=$	8884933102832021670310856601112383279507496491807071433260928721853918699951
n	$=$	8884933102832021670310856601112383279454437918059397120004264665392731659049
$a4$	$=$	2481513316835306518496091950488867366805208929993787063131352719741796616329
$a6$	$=$	4387305958586347890529260320831286139799795892409507048422786783411496715073
$r4$	$=$	5473953786136330929505372885864126123958065998198197694258492204115618878079
$r6$	$=$	5831273952509092555776116225688691072512584265972424782073602066621365105518
gx	$=$	7638166354848741333090176068286311479365713946232310129943505521094105356372
gy	$=$	762687367051975977761089912701686274060655281117983501949286086861823169994
r	$=$	8094458595770206542003150089514239385761983350496862878239630488323200271273

3 Elliptic curves in Edwards form

We are looking for curves such that

$$x^2 + y^2 = 1 + d * x^2 * y^2,$$

where d is a non-square in $\mathbb{F}_p$ (this condition is to get a complete addition formula). We choose p such that $p \equiv 3 \mod 4$. This condition implies that all the Montgomery curves are Ewards curves. The coefficient d (non-square) is the hash of a random number rd. In the case of Edwards curves, the number n of rational points cannot be prime : there is always an element of order 4. Then we try to obtain a group of order $n = 4u$ where u is prime. A point $g = (gx, gy)$ (not of low order 1,2,4) is given. This point can be of order $n/2^t$ where $t = 0, 1, 2$. Using this point, points of order n, $n/2$, $n/4$ can be computed :

1. if g is of order n, $2g$ is of order $n/2$ and $4g$ is of order $n/4$;
2. if g is of order $n/2$, $2g$ is of order $n/4$ and $g + (0, -1)$ is of order n ;
3. if g is of order $n/4$, $g + (0, -1)$ is of order $n/2$ and $g + (1, 0)$ is of order n.

Then the file descriptor of such a curve contains 8 lines defining the parameters p,n,d,rd,gx,gy,r,t.

p	$=$	17788785049862795200150516910406025137463828480015848539718291306993861084899
n	$=$	17788785049862795200150516910406025137363578126680481424741935402610840792044
d	$=$	3796951610952418946414838013946402540659352227509671351658573117542984656493
rd	$=$	8691808718684137624443735665996936692240583232324910500040371199339620074813
gx	$=$	1986605118669389278383185019082317115767420240937840666424031679646376737334
gy	$=$	13522141226273509754871071682844347818526232922984052207011535368467814622472
r	$=$	11437956621720228291212199612953420381679188428091051450834331532002067513477
t	$=$	2

4 Elliptic curves in Montgomery form

Now we are looking for curves such that

$$B * y^2 = x^3 + A * x^2 + x.$$

We know that any Edwards curve is birationally equivalent over $\mathbb{F}_p$ to a Montgomery curve. When $p = 4k + 3$, the converse is true. Then in this case we do not choose special Montgomery curves by computing these curves from random Edwards curves. To fill in the Montgomery part of the database, we have just transformed the Edwards curves of the database :

$$A = \frac{2 * (1 + d)}{(1 - d)} \quad B = \frac{4}{(1 - d)},$$

$$d = \left(1 - \frac{4}{B}\right).$$

Recall that the number of $\mathbb{F}_p$-rational points of the curve is $n = 4 * u$ where u is a prime number.

We also compute also $G = (u, v)$, the transform of $g = (x, y)$ by

$$u = \frac{(1+y)}{(1-y)} \quad v = \frac{(1+y)}{(1-y)x}.$$

Then to verify that the curve is not choosen but draw at random, we have to compare the hash of rd to $\left(1 - \frac{4}{B}\right)$ and the hash of r to $\frac{u}{v}$. Then the file descriptor of such a curve contains 9 lines defining the parameters p,n,rd,A,B,gx, gy,r,t. Remark that now $g = (gx, gy)$ is a point satsfying the Montgomery equation. This point is obtained from a point (also called g) satisfying the Edwards equation by the preceding transform.

$$\begin{array}{rcl}
p & = & 17788785049862795200150516910406025137463828480015848539718291306993861084899 \\
n & = & 17788785049862795200150516910406025137363578126680481424741935402610840792044 \\
rd & = & 8691808718684137624443735665996936692240583232324910500040371199339620074813 \\
A & = & 13281829785455600117986773687472126603142374585246151870662508733041038873290 \\
B & = & 13281829785455600117986773687472126603142374585246151870662508733041038873292 \\
gx & = & 868693958471480657503045071070474722468026101269185396611087417702398543012 \\
gy & = & 9629180621892378213082525929766132327431100380190226639157652543015175391821 \\
r & = & 11437956621720228291212199612953420381679188428091051450834331532002067513477 \\
t & = & 2
\end{array}$$

5 The size p of the curves

The curves are curves defined on the prime field $\mathbb{F}_p$ where p is a prime of size about 160, 192, 256, 384, 512 bits. More precisely as we draw bits at random, it may happen that one or more most significants bits are 0. In this case the size of p is not exactly the designed size but one or more bits less. Note that in each case ther are curves reaching the designed size (about half of them !).

6 Use of the database

The name of the data base is **Arcana-ECDB**. Each curve of the database has a name. For exemple e512-007 (the Edward curve of size 512 and number 007) which is described by the file e512-007.gp, or w384-013 (the Weierstrass curve of size 384 and number 013).