Elliptic curves satisfying the Brainpool standard criteria and the twist security.

Rafal Gliwa and Janusz Szmidt

ECC 2015, rump session

Bordeaux, 28 IX 2015

The Brainpool Standard

- ECC Brainpool Standard Curves and Curves Generation, v. 1.0. 2005.
- Request for Comments 9639, 2010.
- www.safecurves.cr.yp.to

- Let *p > 3* be a prime number and let *E* be an elliptic curve $\boldsymbol{y^2 = x^3 + Ax + B}$ over the finite field $\boldsymbol{F_p}$
- We search for elliptic curves over $\boldsymbol{F_p}$ for *p* being randomly chosen prime number of the lengths of 384 and 512 bits, satisfying the Brainpool Standard criteria and the twist security.

The Brainpool Standard Criteria

- The order $q = \#E$ of an elliptic curve is a prime number $q < p$.
- The Tate–Weil bound $l > 100$, where l is t*he* degree of the extension $GF(p^l)$ of the basic field, where the cyclic group E is embedded:

$$l = \min\{t : q \mid p^t - 1\}$$

- The class number of the maximal order of the endomorphism ring *End(E) of the elliptic curve E* is > 10 000 000.

The twist security

Let *E'* be a quadratic twist of the elliptic curve *E.* Then we have for the orders of the curves:

$$\#E + \#E' = 2p + 2$$

The twist criterion we have chosen is a condition, that **the order #E' of the twisted curve has a prime factor which is > 2^{200}**.

It was stated on www.safecurve.cr.yp.to, that the recommended curves given in the Brainpool Standard do not satisfy the twist security.

Example 1: L = 384 bits

The Brainpool Standard Criteria

p =
0x8926CF966048CB248C02D815BFC2445A3A12F246BF7D7C17201890D351FD312C878DB307
8617E8C9BC1008155BBD1957;

seed = 0xFF8606C4CF0291732361834766 5ED4E4E920E4F1;

A =
0x7F635297C23DFC716BD71FC3840CF1720E5E7B4965388C3C079DF7B95EFC1C51473852A3\C1
31BD71DD2100005227DDDF;

B =
0x65388C3C079DF7B95EFC1C51473852A3C131BD71DD2100005227DDDF631942B65BC7EE6ECE
981CF928E772F396709047;

#E =
0x8926CF966048CB248C02D815BFC2445A3A12F246BF7D7C170867AA95DBF2A5EE69D699A0\A
0BB8371D5495783CF3E43B9;

h = 1;

Example 1: L=384 bits, cont.

#E_Twist =

0x8926CF966048CB248C02D815BFC2445A3A12F246BF7D7C1737C97710C807BC6AA\
544CC6E6B744E21A2D6B8A6E83BEEF7;

Factorization of #E_Twist:

[<1223, 1>, <266541821383, 1>,
<647571080897359108708620335857456732540609306 9\
268237656796639470608037243785381325260539016286055146 3, 1>]

The largest factor: 335 bits.

Example 2: L = 512 bits

p =
0x8BA7A1DA4A560F3680DA05C5974B485C70A1F8B9D8C06709C9D28CE36D4D49B02BFA5C24B
CF77C96AAC029F0D52A19DAB519E0D17463DA9ACF17583D0C60108F;

A =
0x89F3686984392B07CEAEA308F3A79EDA402C20BFFD1337BE883BB7205CA4614C759F1848FC5
04463E2CC22DC9E6EFB989BA7C07C8E1DE2EC2F2FBF3F308069C6;

B =
0x5FF93B66D906691C893188D94369109DCF2E6C3B9EE52F7194FCE4BA999E6C18E6F73109316
6CC169C841690486FFA023F4FD6702B2229FC299206C2ABFCD3B3;

#E =
0x8BA7A1DA4A560F3680DA05C5974B485C70A1F8B9D8C06709C9D28CE36D4D49B00FE44231FB
13F25BEB328831B5AC5A220D18A928557CF74EB8465DF45D54541F;

h = 1;

Example 2: L = 512 bits, cont.

#E_Twist =
0x8BA7A1DA4A560F3680DA05C5974B485C70A1F8B9D8C06709C9D28CE36D4D49B04
81076177EDB06D16A4DCBAFF4A7D9935D1B187A934ABDE6E5E85285BB6BCD01;

Factorization of #E_Twist:

[<607, 1>, <376823, 1>, <24738795675333193, 1>,
<19164945483752000708269053541789, 1>,
<67446821492019875251826964766377471156156804043234199904741093767390
328613909399162293926488236229, 1>]

The largest factor: 325 bits.