

Internet Draft
<[draft-ladd-safecurves-01.txt](#)>
Category: Informational
Expires 9 July 2014

W. Ladd
Grad Student
UC Berkeley
8 January 2014

Additional Elliptic Curves for IETF protocols
<[draft-ladd-safecurves-01.txt](#)>

Status of this Memo

Distribution of this memo is unlimited.

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on 9 July 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This internet draft contains curves whose Jacobians are groups over

which the Decisional Diffie-Hellman problem is hard, and which have implementation advantages.

Table of Contents

1. Introduction	3
2. The curves	3
3. Explicit Formulas	4
4. Security Considerations	4
5. IANA Actions	5

[1. Introduction](#)

This document contains a set of elliptic curves over prime fields with many security and performance advantages. They are twist-secure, have large prime order subgroups, high embedding degree, endomorphism rings of large discriminant, and primes of fast shapes.

These curves have been generated in a rigid manner by computer search. As such there is very little risk that these curves were selected to exhibit weaknesses to attacks not in the open literature. The field is the only free choice, and in all circumstances has been picked to enable highly efficient arithmetic. Proofs of all properties claimed exist in [[SAFECURVES](#)].

[2. The Curves](#)

Each curve is given by an equation and a basepoint, together with an order. All curves are elliptic. Validation information is given at [[SAFECURVES](#)]. The names given in this document indicate the family. The basepoint is given as an (x,y) ordered pair.

Curve25519 is a curve over $\text{GF}(2^{255}-19)$, formula $y^2=x^3+486662x^2+x$, basepoint (9, 14781619447589544791020593568409986887264606134616475288964881837755586237401), order $2^{252} + 27742317777372353535851937790883648493$.

E382 is a curve over $\text{GF}(2^{382}-105)$, formula $x^2+y^2=1-67254x^2y^2$, basepoint (3914921414754292646847594472454013487047137431784830634731377862923477302047857640522480241298429278603678181725699, 17), order $2^{380} - 1030303207694556153926491950732314247062623204330168346855$

M383 is a curve over $\text{GF}(2^{383}-187)$, formula $y^2=x^3+2065150x^2+x$, basepoint (12, 4737623401891753997660546300375902576839617167257703725630389791524463565757299203154901655432096558642117242906494), order $2^{380} + 166236275931373516105219794935542153308039234455761613271$

Curve3617 is a curve over $\text{GF}(2^{414}-17)$, formula $x^2+y^2=1+3617x^2y^2$, basepoint

(17319886477121189177719202498822615443556957307604340815256226
 171904769976866975908866528699294134494857887698432266169206165, 34),
 order 2^{411} -
 33364140863755142520810177694098385178984727200411208589594759

M511 is a curve over $GF(2^{511}-187)$, formula $y^2 = x^3 + 530438x^2 + x$,
 basepoint (5,
 25004106455650724233689811491392132522115686851736085900709792642
 48275228603899706950518127817176591878667784247582124505430745177
 116625808811349787373477), order $2^{508} +$
 107247547596357476240445315140681218420707566274348330289655408
 08827675062043

E521 is a curve over $GF(2^{521}-1)$, formula $x^2 + y^2 = 1 - 376014x^2y^2$,
 basepoint
 (1571054894184995387535939749894317568645297350402905821437625
 18115230499438118852963259119606760410077267392791511426719338990
 5003276673749012051148356041324, 12), order 2^{519} -
 3375547632585017057891076304187826360719049612140512266186351500
 85779108655765

3. Explicit Formulas

On Montgomery curves, curves of the form $y^2 = x^3 + Ax^2 + x$, the typical technique is to work over the Kummer curve instead, i.e. drop y coordinates for use in Diffie-Hellman. Let (X_1, Z_1) , (X_2, Z_2) , (X_3, Z_3) be coordinates such that X_i/Z_i is the x -coordinate of P_i , with $P_i = [i]P_1$ on the curve. Then

$$\begin{aligned} X_5 &= Z_1((X_3 - Z_3)(X_2 + Z_2) + (X_3 + Z_3)(X_2 - Z_2))^2 \\ Z_5 &= X_1((X_3 - Z_3)(X_2 + Z_2) - (X_3 + Z_3)(X_2 - Z_2))^2 \\ X_4 &= (X_2 + Z_2)^2(X_2 - Z_2) \\ Z_4 &= (4X_2^2Z_2)((X_2 - Z_2)^2 + a24(4X_2^2Z_2)) \end{aligned}$$

gives X_i/Z_i as the x coordinate of P_i for i in $\{4, 5\}$ where $a24 \cdot 4 = A + 2$

On Edwards curves, curves of the form, $x^2 + y^2 = 1 + dx^2y^2$ a complete addition formula, which works for doubling as well, is given by representing points as $x = Z/X$, $y = Z/Y$. The formula for adding (X_1, Y_1, Z_1) to (X_2, Y_2, Z_2) yielding (X_3, Y_3, Z_3) is then

$$\begin{aligned} A &= Z_1Z_2 \\ B &= dA^2 \\ C &= X_1X_2 \\ D &= Y_1Y_2 \\ E &= C \cdot D \\ H &= C - D \\ I &= (X_1 + Y_1)(X_2 + Y_2) - C - D \\ X_3 &= c(E + B) \cdot H \end{aligned}$$

Ladd, Watson

Expires 9 July 2014

[Page 4]

$$Y3 = c*(E-B)*I$$
$$Z3 = A*H*I$$

These formulas are from the [\[EFD\]](#).

Using these formulas the standard double-and-add or Montgomery ladder recurrence can be used to compute multiples of points.

The Montgomery curve formulas require only the x coordinate. Protocols based on ECDH should give strong consideration to transmitting only the x coordinate, in which case no validation is required. The above addition formulas cannot be used to add points on Montgomery curves, as they ignore the y coordinate entirely.

It is highly recommended that Edwards curve points are transmitted in compressed form to avoid implementations with missing curve membership checks from working. The canonical compression is the y coordinate, followed by an indicator of the low bit of the x coordinate. Formulas for decompression are left as an exercise to the reader.

[4. Security Considerations](#)

This entire document discusses methods of implementing cryptography securely. The time for an attacker to break the DLP on these curves is the square root of the group order with the best known attacks. These curves are twist-secure, avoiding the need for some checks in some protocols.

It is recommended that implementors use the Montgomery ladder on Montgomery curves with x coordinate only to avoid side-channel attacks when Diffie-Hellman is being used. In this mode, curve checks are not required. Otherwise standard curve (but not group) membership checks are required for ECDH to be secure.

These curves are complete, avoiding certain attacks against naive implementations of ECC protocols. They have cofactor greater than one, occasionally requiring slight adjustments to protocols.

This is not an exhaustive discussion of security considerations relating to the implementation of these curves. Implementors must be familiar with cryptography to safely implement any cryptographic standard, and this standard is no exception.

[4. IANA Considerations](#)

IANA should maintain a registry of these curves, calling them `chicagocurve-XXXX` where XXXX is the curve identifier.

5. References

[SAFECURVES] safecurves.cr.yp.to

[EFD] <http://www.hyperelliptic.org/EFD/g1p/index.html>

Author's Address

Watson Ladd
watsonbladd@gmail.com
Berkeley, CA