A note on high-security general-purpose elliptic curves

Diego F. Aranha[1], Paulo S. L. M. Barreto[2⋆], and Geovandro C. C. F. Pereira[2]

[1] Computer Science Dept, University of Brasília.
E-mail: dfaranha@unb.br
[2] Escola Politécnica, University of São Paulo.
E-mails: {pbarreto,geovandro}@larc.usp.br

Abstract. In this note we describe some general-purpose, high-efficiency elliptic curves targeting at security levels beyond 2^{128}. As a bonus, we also include legacy-level curves. The choice was made to facilitate state-of-the-art implementation techniques.

1 Introduction

General-purpose elliptic curves are necessary to attain high-efficiency implementations of the most common cryptographic protocols like asymmetric encryption and plain digital signatures (but setting aside less conventional application like identity-based encryption). The standard NIST curves [11], though fairly efficient overall, arguably no longer represent the state of the art in the area [4, 6].

More efficient general-purpose curves have been recently proposed to address this situation [3, 4, 7], but for the 2^{128} security level at most, which corresponds to the expected security level of the standard NIST curve P-256. This is the case of Curve25519 [3] and Curve1174 [4]. However, while there is reason to look for higher security curves [12], no similar curves seem to have been proposed in the literature for higher security levels, matching the presumed levels of (say) the standard NIST curves P-384 and/or P-521.

In this short note we address this need up to the expected security level of P-384, adopting the same settings as Curve25519 and Curve1174, respectively.

⋆ Supported by CNPq research productivity grant 306935/2012-0.

2 Curve choice

The curves Curve25519 and Curve1174 have been engineered to facilitate simple, efficient and secure implementation of general-purpose elliptic curve cryptosystems, with impressive results [7] and many useful properties, like the indistinguishability of points from uniform random strings and many others [4]. On these grounds, it makes sense to look for similar curves at higher security levels. At the same time, one can take the opportunity to provide legacy-level curves as well, matching e.g. the expected security level of the standard NIST curve P-224.

Curve25519 [3] is an Elligator type 2 curve with the following properties (among others):

- It is a Montgomery curve [10] over a large prime field $\mathbb{F}_p$;
- The prime p has the form $p = 2^m - \delta$ where $0 < \delta < \lceil \lg(p) \rceil = m$;
- The prime p satisfies $p \equiv 5 \pmod 8$, hence square root computation in $\mathbb{F}_p$ can be done with the Atkin method [2];
- The value $\xi = 2$ is a quadratic non-residue in $\mathbb{F}_p$, and hence can used to define a non-trivial quadratic twist of an elliptic curve over $\mathbb{F}_p$;
- The curve equation is $E : y^2 = x^3 + Ax^2 + x$ and the twist equation is $E' : v^2 = u^3 + 2Au^2 + 4u$, where $A > 2$ is as small as possible.
- The curve order has the form $n = 8r$ where r is prime;
- The order of the non-trivial quadratic twist of the curve has the form $n' = 4r'$ where r' is prime, with $|r'| = |r| + 1$;

Curve1174 [4] is an Elligator type 1 curve with the following properties (among others):

- It is an Edwards curve [5, 8] over a large prime field $\mathbb{F}_p$;
- The prime p has the form $p = 2^m - \delta$ where $0 < \delta < \lceil \lg(p) \rceil = m$;
- The prime p satisfies $p \equiv 3 \pmod 4$, hence square root computation in $\mathbb{F}_p$ can be done with the Cippolla-Lehmer method [9];
- The curve equation is $E : x^2 + y^2 = 1 + dx^2y^2$ and the equation of a non-trivial quadratic twist of E is $E' : u^2 + v^2 = 1 + (1/d)u^2v^2$, where $d > 1$ is as small as possible;
- The curve order has the form $n = 4r$ where r is prime;
- The order of the non-trivial quadratic twist of the curve has the form $n' = 4r'$ where r' is prime, with $|r'| = |r|$;

3 The curves

We now list curves for several security levels, up to the level roughly comparable to the presumed security level of the NIST curve P-384. The primes have the general form $p = 2^m - \delta$ for δ as small as possible. While it would be desirable that $\delta < 32$ (see [4]), this is not always possible. Yet, insisting that $\delta < \lg p$ increases the likeliness that any attack advantage this setting might cause is negligible (exponentially small). An additional practical constraint is that the value of δ fits one byte, to facilitate the detection of values outside the valid range is this is deemed necessary.

Table 1 contains Montgomery curves, while Table 2 contains Edwards curves. For completeness, we include the original Curve25519 and Curve1174.

Table 1. Montgomery curves

curve	p	A	$\lvert r\rvert$	security
Curve22103	$2^{221} - 3$	204400	218	2^{109}
Curve25519	$2^{255} - 19$	486662	252	2^{126}
Curve383187	$2^{383} - 187$	229969	380	2^{190}

Table 2. Edwards curves

curve	p	$-d$	$\lvert r\rvert$	security
Curve4417	$2^{226} - 5$	4417	224	2^{112}
Curve1174	$2^{251} - 9$	1174	249	2^{124}
Curve67254	$2^{382} - 105$	67254	380	2^{190}

A proof-of-concept implementation of all these curves is available as part of the RELIC library [1]. Work on a production-quality implementation is ongoing.

4 Conclusion

We have described general-purpose high-efficiency curves roughly matching the expected security of the standard NIST curve P-384. As a bonus, we also provided legacy-level curves roughly matching

the expected security of the standard NIST curve P-224. All curves follow the Elligator 1 and 2 strategy, which is arguably the state of the art for the design of cryptographically-oriented elliptic curves.

This is work in progress. Better curves may be suggested as they become available.

References

1. D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient LIbrary for Cryptography. `http://code.google.com/p/relic-toolkit/`.
2. O. Atkin. Square roots and cognate matters modulo $p = 8n + 5$. Number Theory mailing list, 1992. `http://listserv.nodak.edu/scripts/wa.exe?A2=ind9211&L=nmbrthry&O=T&P=562`.
3. Dan J. Bernstein. Curve25519: New Diffie-Hellman speed records. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography – PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 207–228. Springer, 2006.
4. Dan J. Bernstein, M. Hamburg, A. Krasnova, and T Lange. Elligator: Elliptic-curve points indistinguishable from uniform random strings. IACR Cryptology ePrint Archive, report 2013/325, 2013.
5. Dan J. Bernstein and Tanja Lange. Security dangers of the NIST curves. In K. Kurosawa, editor, *Advances in Cryptology – Asiacrypt 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.
6. Dan J. Bernstein and Tanja Lange. Security dangers of the NIST curves. Invited talk, International State of the Art Cryptography Workshop, Athens, Greece, 2013.
7. Dan J. Bernstein, Tanja Lange, and Peter Schwabe. The security impact of a new cryptographic library. In Alejandro Hevia and Gregory Neven, editors, *Latincrypt 2012*, volume 7533 of *Lecture Notes in Computer Science*, pages 159–176. Springer, 2012.
8. Harold M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.
9. D. H. Lehmer. Computer technology applied to the theory of numbers. In W. J. LeVeque, editor, *Studies in Number Theory*. Mathematical Association of America, 1969.
10. P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48:243–264, 1987.
11. National Institute of Standards and Technology – NIST. *Federal Information Processing Standard (FIPS 186-4) – Digital Signature Standard (DSS)*, July 2013.
12. National Security Agency – NSA. *Suite B Cryptography / Cryptographic Interoperability*, January 2009. `http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml`.