Four$\mathbb{Q}$

Four-dimensional decompositions on a $\mathbb{Q}$-curve

http://research.microsoft.com/fourqlib

Craig Costello and **Patrick Longa**
Microsoft Research

Four$\mathbb{Q}$: pulling together the state-of-the-art in ECC

- CM endomorphism [GLV01]
- Frobenius ($\mathbb{Q}$-curve) endo [GLS09, Smi13, GI13]

- Edwards form [Edw07]
- Efficient Edwards coord. [BBJ+08, HCW+08]

- Arithmetic over the Mersenne prime $p = 2^{127} - 1$

Four$\mathbb{Q}$

This powerful combination brings in simplicity and flexibility, and enables ***the fastest*** *curve-based computations to date.*

FourQ
in the news

The Register® Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS WEEKEND

Security

Microsoft throws crypto foes an untouchable elliptic curveball

Redmond's new, free, crypto library dubbed FourQ leaves P-256 swinging and missing

15 Sep 2015 at 03:58, Richard Chirgwin   24   42

While Washington mulls ways to make crypto less effective, the industry, thank heavens, continues to push in the other direction. Microsoft Research has just published an elliptic curve library it reckons is considerably faster than what's currently available.

Outlined in this International Association for Cryptologic Research (IACR) paper, the implementation, the

More like this

Cryptography   Nist

Most read

Confession: I was a teenage computer virus writer

VANISHED GLOBAL WARMING may NOT RETURN – UK Met Office

PRIMITIVE TOOLS found near MICROSOFT headquarters

World finally ready for USB-bootable OS/2

The Curve

$$E/\mathbb{F}_{p^2}: -x^2 + y^2 = 1 + dx^2y^2,$$

with $p = 2^{127} - 1$, $d = 125317048443780598345676279555970305165i + 4205857648805777768770$, $\#E = 392 \cdot N$, where N is a 246-bit prime.

- Provides ~ 122.5 bits of security.
- Fastest (large char) ECC addition laws are complete on E.
- E is a degree-2 $\mathbb{Q}$-curve: endomorphism ψ.
- E has CM by order of $D = -40$: endomorphism ϕ.
- $\psi(P) = [\lambda_\psi]P$ and $\phi(P) = [\lambda_\phi]P$ for all $P \in E[N]$ and $m \in [0, 2^{256}]$

$$m \mapsto (a_1, a_2, a_3, a_4)$$

$$[m]P = [a_1]P + [a_2]\phi(P) + [a_3]\psi(P) + [a_4]\psi(\phi(P))$$

Four$\mathbb{Q}$lib: an efficient and secure ECC library for Four$\mathbb{Q}$

Version 1.0 recently released:

- Supports core ECC functions.
- Fully protected against timing and cache attacks.
- Wide platform support (e.g., ARM, x86 and x64) using Windows and Linux: includes a portable implementation in C and optimized x64 implementations.
- Option to disable the use of the endomorphisms ψ and ϕ.

Comparison with other 128-bit security curves

Cycles to compute variable-base scalar multiplication (in 10^3 cycles)

Curve	Field	Intel Atom	Intel S Bridge	Intel I Bridge	Intel Haswell	AMD Kaveri
Four$\mathbb{Q}$ (this work)	$\mathbb{F}_{p^2},\ p = 2^{127} - 1$	**442**	**74**	**71**	**59**	**122**
Kummer (Gaudry-Schost)	$\mathbb{F}_{p},\ p = 2^{127} - 1$	556	89	88	61	151
GLV+GLS (Longa-Sica)	$\mathbb{F}_{p^2},\ p = 2^{128} - 5997$	-	92	89	-	-
GLS binary (Hankerson-Karabina-Menezes)	$\mathbb{F}_{2^{254}}$	-	120	114	62	-
Curve25519 (Bernstein)	$\mathbb{F}_{p},\ p = 2^{255} - 19$	1,109	157	159	162	301
NIST P-256	$\mathbb{F}_{p},\ p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$	-	400	-	312	-

Kummer: implementations by Bos et al [BCH+13] and Bernstein et al [BCL+14]. Results from [eBACS].
GLV+GLS: implementation and results from Faz Hernandez-Longa-Sanchez [FLS15].
GLS binary: implementation by Oliveira et al [OLA+14]. Results from [eBACS].
Curve25519: implementations by Bernstein et al [BDL+11] and Chou [Cho14]. Results for [BDL+11] from [eBACS].
NIST P-256: implementation and results from Gueron-Krasnov [GK15].

Final thoughts

- Four$\mathbb{Q}$ is 4–5x faster than NIST P-256, 2–3x faster than Curve25519.

- Even without using endomorphisms ψ and ϕ, Four$\mathbb{Q}$ is still ~3x faster than NIST P-256 and up to 1.5x faster than Curve25519.

Links

- “Four$\mathbb{Q}$: four-dimensional decompositions on a Q-curve over the Mersenne prime”. ASIACRYPT 2015 (to appear).

  Extended paper version:

  http://eprint.iacr.org/2015/565

- Four$\mathbb{Q}$lib, version 1.0

  http://research.microsoft.com/fourqlib/

References

[Ber06] D.J. Bernstein. Curve25519: New Diffie-Hellman speed records. PKC 2006.

[BBJ+08] D.J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters. Twisted Edwards curves. AFRICACRYPT 2008.

[BCL+14] D. J. Bernstein, C. Chuengsatiansup, T. Lange and P. Schwabe. Kummer strikes back: New DH speed records. ASIACRYPT 2014.

[BDL+11] D.J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang. High-speed high-security signatures. CHES 2011.

[eBACS] D.J. Bernstein and T. Lange. eBACS: ECRYPT Benchmarking of Cryptographic Systems, accessed on May 19, 2015. http://bench.cr.yp.to/results-dh.html

[BCH+13] J.W. Bos, C. Costello, H. Hisil and K. Lauter. Fast cryptography in genus 2. EUROCRYPT 2013.

[Cho14] T. Chou. Fastest Curve25519 implementation ever. NIST Workshop on Elliptic Curve Cryptography Standards, 2015.

[Edw07] H. Edwards. A normal form for elliptic curves. Bulletin of the AMS, 2007.

[FLS15] A. Faz-Hernandez, P. Longa, and A.H. Sanchez. Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV-GLS curves (extended version). J. Cryptographic Engineering, 2015.

[GLS09] S.D. Galbraith, X. Lin, M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. EUROCRYPT 2009.

[GLV01] R.P. Gallant, R.J. Lambert, S.A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. CRYPTO 2001.

[GS12] P. Gaudry and E. Schost. Genus 2 point counting over prime fields. J. Symbolic Computation, 2012.

[GK15] S. Gueron and V. Krasnov. Fast prime field elliptic curve cryptography with 256 bit primes. J. Cryptographic Engineering, 2015.

[GI13] A. Guillevic and S. Ionica. Four-dimensional GLV via the Weil restriction. ASIACRYPT 2013.

[HKM09] D. Hankerson, K. Karabina and A. Menezes. Analyzing the Galbraith-Lin-Scott Point Multiplication Method for Elliptic Curves over Binary Fields. IEEE Transactions on Computers, 2009.

[HCW+08] H. Hisil, G. Carter, K.K. Wong and E. Dawson. Twisted Edwards curves revisited. ASIACRYPT 2008.

[OLA+14] T. Oliveira, J. Lopez, D. F. Aranha, and F. Rodriguez-Henriquez. Two is the fastest prime: Lambda coordinates for binary elliptic curves. J. Cryptographic Engineering, 2014.

[Smi13] B. Smith. The Q-curve construction for endomorphism-accelerated elliptic curves. J. Cryptology (to appear), 2015.