Complete addition formulas for prime order elliptic curves

Joost Renes[1] Craig Costello[2] Lejla Batina[1]

[1]Radboud University, Digital Security, Nijmegen, The Netherlands
j.renes,lejla@cs.ru.nl
[2]Microsoft Research, Redmond, USA
craigco@microsoft.com

9th May 2016

Outline

- Elliptic curve preliminaries
- Problem of exceptional cases
- Complete addition formulas
- Comparison of results

$E(k)$: elliptic curve over a field k with $\mathrm{char}(k) \neq 2, 3$

Every elliptic curve can be written in short Weierstrass form

- Embedded in $\mathbb{P}^2(k)$ as $E : Y^2Z = X^3 + aXZ^2 + bZ^3$
- The point $\mathcal{O} = (0 : 1 : 0)$ is called the point at infinity
- Affine points $(x : y : 1)$ given by $y^2 = x^3 + ax + b$

- The points on E form an abelian group under point addition $\oplus$ (with neutral element $\mathcal{O}$)
- Scalar multiplication $(k, P) \mapsto [k]P$ $(k \in \mathbb{Z}, P \in E)$
- The order of E is its order as a group

Elliptic curve cryptography (ECC)

Elliptic curve discrete logarithm problem (ECDLP)

Given two points $P, Q \in E$ such that $Q \in \langle P \rangle$. Find $k \in \mathbb{Z}$ such that $Q = [k]P$.

Commonly k is a secret, Q is public

- Key exchange: ECDH
- Signatures: ECDSA, EdDSA

Weierstrass model

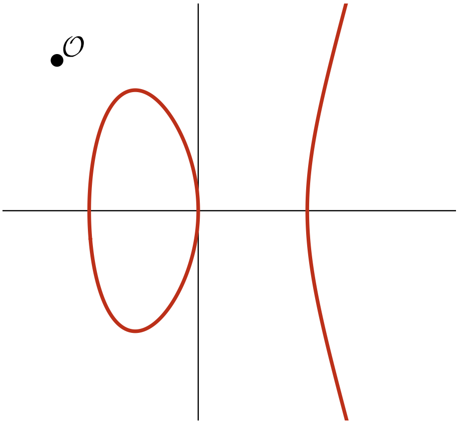

Figure: $E/\mathbb{R} : y^2 = x^3 + ax + b$

Chord and tangent addition

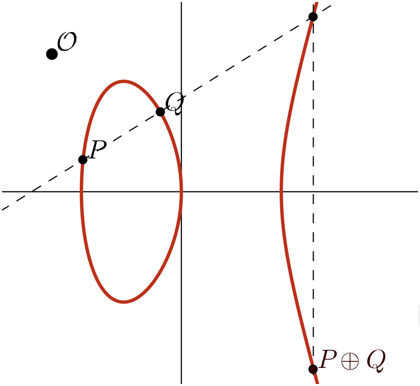

Figure: $E/\mathbb{R} : y^2 = x^3 + ax + b$

- if $P \neq \pm Q$
- if $P \neq \mathcal{O}$
- if $Q \neq \mathcal{O}$

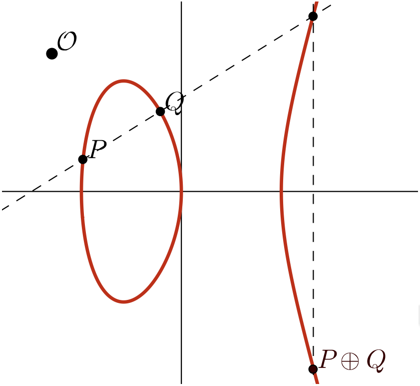

Figure: $E/\mathbb{R} : y^2 = x^3 + ax + b$

Weierstrass model doubling

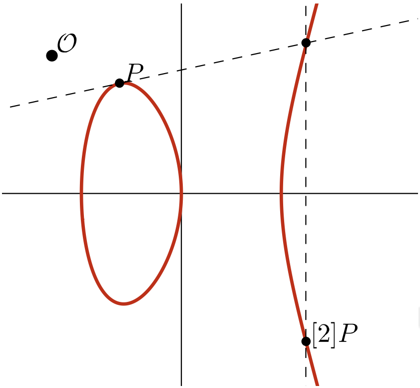

Figure: $E/\mathbb{R} : y^2 = x^3 + ax + b$

Weierstrass model doubling

- if $P \neq \mathcal{O}$

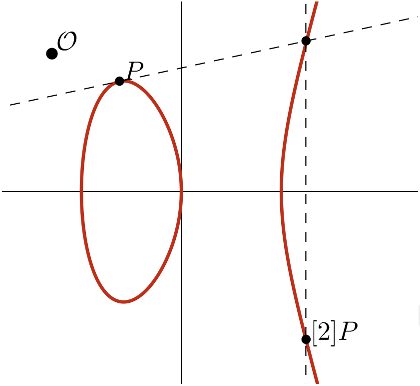

Figure: $E/\mathbb{R} : y^2 = x^3 + ax + b$

Implementation (Homogeneous addition)

$(X_1 : Y_1 : Z_1) \oplus (X_2 : Y_2 : Z_2) = (X_3 : Y_3 : Z_3)$, where:

$$\begin{aligned}
X_3 &= (X_2Z_1 - X_1Z_2)\Big[(Y_2Z_1 - Y_1Z_2)Z_1Z_2 \\
&\quad - (X_2Z_1 - X_1Z_2)^3 - 2(X_2Z_1 - X_1Z_2)X_1Z_2\Big], \\
Y_3 &= (Y_2Z_1 - Y_1Z_2)\Big[3(X_2Z_1 - X_1Z_2)X_1Z_2 - (Y_2Z_1 - Y_1Z_2)Z_1Z_2 \\
&\quad + (X_2Z_1 - X_1Z_2)^3\Big] - (X_2Z_1 - X_1Z_2)^3Y_1Z_2, \\
Z_3 &= (X_2Z_1 - X_1Z_2)^3Z_1Z_2.
\end{aligned}$$

But: $\left.\begin{array}{l} P = Q \\ P = \mathcal{O} \\ Q = \mathcal{O} \end{array}\right\} \implies X_3 = Y_3 = Z_3 = 0$ (**not in $\mathbb{P}^2$!**)

Implementation (Homogeneous doubling)

$[2](X : Y : Z) = (X_3 : Y_3 : Z_3)$, where

$$
\begin{aligned}
X_3 &= 2\Big[(aZ^2 + 3X^2)^2 - 8XY^2Z\Big]YZ,\\
Y_3 &= (aZ^2 + 3X^2)\Big[12XY^2Z - (aZ^2 + 3X^2)^2\Big] - 8Y^4Z^2,\\
Z_3 &= 8Y^3Z^3.
\end{aligned}
$$

<u>But:</u> $P = \mathcal{O} \implies X_3 = Y_3 = Z_3 = 0$ (**<u>not in $\mathbb{P}^2$!</u>**)

Exceptional cases

- Curves implemented using formulas with exceptional cases
- Handled by if-statements:
  - Code complexity
  - Bugs
  - Non-time-constant
  - Potential vulnerabilities

Curve model

- Problems appear for curves in short Weierstrass form
- Can deal with the exceptions by changing the model
  - (twisted) Edwards
  - (twisted) Hessian
- Not possible for prime order curves

Prime order curves

- The example curves originally specified in the working drafts of ANSI, versions X9.62 and X9.63 [1, 2].
- The five NIST prime curves specified in FIPS 186-4, i.e. P-192, P-224, P-256, P-384 and P-521.
- The seven curves specified in the German brainpool standard [9], i.e., `brainpoolPXXXr1`, where $\texttt{XXX} \in \{160, 192, 224, 256, 320, 384, 512\}$.
- The eight curves specified by the UK-based company Certivox [8], i.e., `ssc-XXX`, where $\texttt{XXX} \in \{160, 192, 224, 256, 288, 320, 384, 512\}$.
- The three curves specified (in addition to the above NIST prime curves) in the Certicom SEC 2 standard [7]. This includes `secp256k1`, which is the curve used in the Bitcoin protocol.

Complete addition formulas

Addition formulas [5]

Tuple of bihomogeneous polynomials $(X_3 : Y_3 : Z_3)$ such that for all $(P, Q) \in E \times E$ either

1. $(X_3(P,Q) : Y_3(P,Q) : Z_3(P,Q)) = P \oplus Q$, or
2. $(X_3(P,Q) : Y_3(P,Q) : Z_3(P,Q)) = (0 : 0 : 0)$.

- If 2 holds for a pair (P, Q), it is called exceptional
- If 2 holds for none of the pairs (P, Q), the addition formulas $(X_3 : Y_3 : Z_3)$ are called complete

Limitations and possibilities

Known results by Bosma and Lenstra [5] for (equivalence classes of) addition formulas of bidegree (2,2):

Theorem:	over an algebraically closed field $\bar{k}$ there are always exceptional pairs
Consequence:	for complete addition formulas over $\mathbb{F}_p$ we have to make sure the exceptional pairs lie in extension fields (Note that this is what is done for Edwards curves as well)

Theorem:	the set is a 3-dimensional k-vector space
Consequence:	there are $\approx q^3$ addition formulas

Choosing the optimal one

For a basis (A_0, A_1, A_2) of the 3-dimensional space, every addition law can be written as

$$aA_0 + bA_1 + cA_2,$$

for $a, b, c \in \mathbb{F}_q$.

Some intuitive arguments:

- Bosma and Lenstra give a basis in which almost no cross-cancelation occurs, so simply choosing one of their basis elements seems optimal
- One of the basis elements is the only addition law which is complete independent of curve coefficients and base field

Choose this addition law, and heavily optimize it!

Complete addition formulas for odd order elliptic curves. For any two points $P = (X_1 : Y_1 : Z_1)$ and $Q = (X_2 : Y_2 : Z_2)$ we can compute $P + Q = (X_3 : Y_3 : Z_3)$ where

$$\begin{aligned}
X_3 &= (X_1Y_2 + X_2Y_1)(Y_1Y_2 - a(X_1Z_2 + X_2Z_1) - 3bZ_1Z_2) \\
&\quad - (Y_1Z_2 + Y_2Z_1)(aX_1X_2 + 3b(X_1Z_2 + X_2Z_1) - a^2Z_1Z_2), \\
Y_3 &= (Y_1Y_2 + a(X_1Z_2 + X_2Z_1) + 3bZ_1Z_2)(Y_1Y_2 - a(X_1Z_2 + X_2Z_1) - 3bZ_1Z_2) \\
&\quad + (3X_1X_2 + aZ_1Z_2)(aX_1X_2 + 3b(X_1Z_2 + X_2Z_1) - a^2Z_1Z_2), \\
Z_3 &= (Y_1Z_2 + Y_2Z_1)(Y_1Y_2 + a(X_1Z_2 + X_2Z_1) + 3bZ_1Z_2) \\
&\quad + (X_1Y_2 + X_2Y_1)(3X_1X_2 + aZ_1Z_2).
\end{aligned}$$

Exceptional pairs are induced by points of order 2, which by assumption only exist over extension fields.

Operation count

$$\text{any } a: \quad \begin{cases} 12\mathbf{M} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 23\mathbf{a} & P \oplus Q \\ 11\mathbf{M} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 17\mathbf{a} & P \oplus Q, Z_Q = 1 \\ 8\mathbf{M} + 3\mathbf{S} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 15\mathbf{a} & [2]P \end{cases}$$

$$a = -3: \quad \begin{cases} 12\mathbf{M} + 2\mathbf{m_b} + 29\mathbf{a} & P \oplus Q \\ 11\mathbf{M} + 2\mathbf{m_b} + 23\mathbf{a} & P \oplus Q, Z_Q = 1 \\ 8\mathbf{M} + 3\mathbf{S} + 2\mathbf{m_b} + 21\mathbf{a} & [2]P \end{cases}$$

$$a = 0: \quad \begin{cases} 12\mathbf{M} + 2\mathbf{m_{3b}} + 19\mathbf{a} & P \oplus Q \\ 11\mathbf{M} + 2\mathbf{m_{3b}} + 13\mathbf{a} & P \oplus Q, Z_Q = 1 \\ 6\mathbf{M} + 2\mathbf{S} + 1\mathbf{m_{3b}} + 9\mathbf{a} & [2]P \end{cases}$$

- **This work** (addition): $12\mathbf{M} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 23\mathbf{a}$
- **This work** (doubling): $8\mathbf{M} + 3\mathbf{S} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 15\mathbf{a}$
- Bernstein and Lange [3] attempt an addition law which works for all NIST prime curves: $26\mathbf{M} + 8\mathbf{S} + \ldots$
- Brier and Joye [6] develop *unified* formulas, still with exceptions: $11\mathbf{M} + 6\mathbf{S} + \ldots$
- Bos *et al.* [4] study a complete *system* of two addition laws
- Chord-and-tangent Jacobian coordinates addition: $\approx 12\mathbf{M} + 4\mathbf{S} + \ldots$
- Chord-and-tangent Jacobian coordinates doubling: $\approx 4\mathbf{M} + 4\mathbf{S} + \ldots$

A comparison

- **This work** (addition): $12\mathbf{M} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 23\mathbf{a}$
- **This work** (doubling): $8\mathbf{M} + 3\mathbf{S} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 15\mathbf{a}$
- Bernstein and Lange [3] attempt an addition law which works for all NIST prime curves: $26\mathbf{M} + 8\mathbf{S} + \dots$
- Brier and Joye [6] develop *unified* formulas, still with exceptions: $11\mathbf{M} + 6\mathbf{S} + \dots$
- Bos *et al.* [4] study a complete *system* of two addition laws
- Chord-and-tangent Jacobian coordinates addition: $\approx 12\mathbf{M} + 4\mathbf{S} + \dots$
- Chord-and-tangent Jacobian coordinates doubling: $\approx 4\mathbf{M} + 4\mathbf{S} + \dots$

IN DEI NOMINE

A comparison

- **This work** (addition): $12\mathbf{M} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 23\mathbf{a}$
- **This work** (doubling): $8\mathbf{M} + 3\mathbf{S} + 3\mathbf{m_a} + 2\mathbf{m_{3b}} + 15\mathbf{a}$
- Bernstein and Lange [3] attempt an addition law which works for all NIST prime curves: $26\mathbf{M} + 8\mathbf{S} + \ldots$
- Brier and Joye [6] develop *unified* formulas, still with exceptions: $11\mathbf{M} + 6\mathbf{S} + \ldots$
- Bos *et al.* [4] study a complete *system* of two addition laws
- Chord-and-tangent Jacobian coordinates addition: $\approx 12\mathbf{M} + 4\mathbf{S} + \ldots$
- Chord-and-tangent Jacobian coordinates doubling: $\approx 4\mathbf{M} + 4\mathbf{S} + \ldots$

Another comparison: OpenSSL

NIST curve	no. of ECDH operations (per 10s) complete	incomplete	factor slowdown
P-192	35274	47431	1.34x
P-224	24810	34313	1.38x
P-256	21853	30158	1.38x
P-384	10109	14252	1.41x
P-521	4580	6634	1.44x

Table: Number of ECDH operations in 10 seconds for the OpenSSL implementation of the five NIST prime curves. Timings were obtained by running the "`openssl speed ecdhpXXX`" command on an Intel Core i5-5300 CPU @ 2.30GHz, averaged over 100 trials of 10s each.

Hardware implementation

Built on top of Mongomery modular multiplier:

- Uses redundant representation, making additions very fast
  - Great for our formulas, since we have many
- No distinction between multiplications and squarings
  - No negative effect, unlike other formulas
- Multiplications by constants are cheap (if predefined)
  - Good for us, since we have a couple
- Can use multiple multipliers
  - Formulas well parallelizable, so benefit from this

Thanks

Thanks for your attention!

[1] Accredited Standards Committee X9. *American National Standard X9.62-1999, Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm (ECDSA).* Draft at http://grouper.ieee.org/groups/1363/Research/Other.html. 1999.

[2] Accredited Standards Committee X9. *American National Standard X9.63-2001, Public key cryptography for the financial services industry: key agreement and key transport using elliptic curve cryptography.* Draft at http://grouper.ieee.org/groups/1363/Research/Other.html. 1999.

[3] D. J. Bernstein and T. Lange. *Complete addition laws for elliptic curves.* Talk at Algebra and Number Theory Seminar (Universidad Autonomo de Madrid). Slides at http://cr.yp.to/talks/2009.04.17/slides.pdf. 2009.

[4] Joppe W. Bos et al. "Selecting Elliptic Curves for Cryptography: An Efficiency and Security Analysis". In: *J. Cryptographic Engineering* (2015). http://dx.doi.org/10.1007/s13389-015-0097-y. DOI: 10.1007/s13389-015-0097-y.

References II

[5] W. Bosma and H. W. Lenstra. "Complete systems of two addition laws for elliptic curves". In: *Journal of Number theory* 53.2 (1995), pp. 229–240.

[6] E. Brier and M. Joye. "Weierstraß Elliptic Curves and Side-Channel Attacks". In: *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002, Paris, France, February 12-14, 2002, Proceedings*. Ed. by D. Naccache and P. Paillier. Vol. 2274. Lecture Notes in Computer Science. Springer, 2002, pp. 335–345. ISBN: 3-540-43168-3. DOI: 10.1007/3-540-45664-3_24. URL: http://dx.doi.org/10.1007/3-540-45664-3_24.

[7] Certicom Research. *SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0*. http://www.secg.org/sec2-v2.pdf. 2010.

[8] Certivox UK, Ltd. *CertiVox Standard Curves*. http://docs.certivox.com/docs/miracl/certivox-standard-curves. Date accessed: September 9, 2015.

[9] ECC Brainpool. *ECC Brainpool Standard Curves and Curve Generation*. http://www.ecc-brainpool.org/download/Domain-parameters.pdf. 2005.