A gentle introduction to elliptic curve cryptography

Craig Costello

Summer School on Real-World Crypto and Privacy
June 11, 2018
Šibenik, Croatia

Microsoft® Research

Part 1: Motivation

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next-generation ECC

Diffie-Hellman key exchange (circa 1976)

$$q = 1606938044258990275541962092341162602522202993782792835301301$$

$$g = 123456789$$

$g^a \bmod q = 7846737452942265357975459631985270257549969298008577794859 3$

$5600481042932181286674410213424831338026262713942994101287 98 = g^b \bmod q$

$a =$
685408003627063
761059275919665
781694368639459
527871881531452

$b =$
362059131912941
987637880257325
269696682836735
524942246807440

$g^{ab} \bmod q = 437452857085801785219961443000845969831329749878767465041215$

Index calculus

$$\text{solve} \quad g^x \equiv h \pmod{p}$$
$$\text{e.g.} \quad 3^x \equiv 37 \pmod{1217}$$

- factor base $p_i = \{2,3,5,7,11,13,17,19\}$, $\#p_i = 8$
- Find 8 values of k where 3^k splits over p_i, i.e., $3^k \equiv \pm\prod p_i \bmod p$

$\pmod{1217}$

$$\begin{aligned}
3^1 &\equiv 3 \\
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \\
3^{25} &\equiv 5^3 \\
3^{30} &\equiv -2 \cdot 5^2 \\
3^{34} &\equiv -3 \cdot 7 \cdot 19 \\
3^{54} &\equiv -5 \cdot 11 \\
3^{71} &\equiv -17 \\
3^{87} &\equiv 13
\end{aligned}$$

$\pmod{1216}$

$$\begin{aligned}
1 &\equiv L(3) \\
24 &\equiv 608 + 2 \cdot L(2) + L(7) + L(13) \\
25 &\equiv 3 \cdot L(5) \\
30 &\equiv 608 + L(2) + 2 \cdot L(5) \\
34 &\equiv 608 + L(3) + L(7) + L(19) \\
54 &\equiv 608 + L(5) + L(11) \\
71 &\equiv 608 + L(17) \\
87 &\equiv L(13)
\end{aligned}$$

$\pmod{1216}$

$$\begin{aligned}
L(2) &\equiv 216 \\
L(3) &\equiv 1 \\
L(5) &\equiv 819 \\
L(7) &\equiv 113 \\
L(11) &\equiv 1059 \\
L(13) &\equiv 87 \\
L(17) &\equiv 679 \\
L(19) &\equiv 528
\end{aligned}$$

Index calculus

solve $g^x \equiv h \pmod{p}$

e.g. $3^x \equiv 37 \pmod{1217}$

$L(2) \equiv 216$
$L(3) \equiv 1$
$L(5) \equiv 819$
$L(7) \equiv 113$
$L(11) \equiv 1059$
$L(13) \equiv 87$
$L(17) \equiv 679$
$L(19) \equiv 528$

Now search for j such that $g^j \cdot h = 3^j \cdot 37$ factors over p_i

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}$$

$$L(37) \equiv 3 \cdot L(2) + L(7) + L(11) - 16 \pmod{1216}$$
$$\equiv 3 \cdot 216 + 113 + 1059 - 1$$
$$\equiv 588$$

Subexponential complexity $L_p[1/3, (64/9)^{1/3}] = e^{\left((64/9)^{1/3}+o(1)\right)(\ln(p))^{1/3}\cdot(\ln\ln(p))^{2/3}}$

Diffie-Hellman key exchange (circa 2016)

$q =$

58096059953699580628595025333045743706869751763628952366614861522872037309971102257373360445331184072513261577549805174439905295945400471216628856721870324010321116397
06440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580
16186020024749256844815024251530444957718760413642873858099017255157393414625583036640591500086964373205321856683254529110790372283163413859958640669032595972518744716
90595408050123102096390117507487600170953607342349457574162729948560133086169585299583046776370191815940885283450612858638982717634572948835466388795543116154464463301
99254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710
716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$g = 123456789$

$g^a \pmod{q} =$

197496648183227193286262018614250555971909799762533760654008147994875775445667054218578105133138217497206890599554928429450667899476
854668595594034093493637562451078938296960313488696178848142491351687253054602202966247046105770771577248321682117174246128321195678
537631520278649403464797353691996736993577092687178385602298873558954121056430522899619761453727082217823475746223803790014235051396
799049446508224661850168149957401474638456716624401906701394472447015052569417746372185093302535739383791980070572381421729029651639
304234361268764971707763484300668923972868709121665568669830978657804740157916611563508569886847487772676671207386096152947607114559
706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532
6052422101474898256696660124195726100495725510022002932814218768060112310763455404567248761396399633344901857872119208518550803791724

$g^b \pmod{q} =$

411604662069593306683228525653441872410777999220572079993574397237156368762038378332742471939666544968793817819321495269833613169937
986164811320795616949957400518206385310292475529284550626247132930124027703140131220968771142788394846592816111078275196955258045178
705254016469773509936925361994895894163065551105161929613139219782198757542984826465893457768888915561514505048091856159412977576049
073563225572809880970058396501719665853110101308432647427786565525121328772587167842037624190143909787938665842005691911997396726455
110758448552553744288464337906540312125397571803103278271979007681841394534114315726120595749993896347981789310754194864577435905673
172970033596584445206671223874399576560291954856168126236657381519414592942037018351232440467191228145585909045861278091800166330876
4073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$a =$

7147687166405; 9571879053605547396582
692405186145916522354912615715297097
100679170037904924330116019497881089
087696131592831386326210951294944584
4004974889298038584931918128447572321
023987160439062006177648318875457556
2337708539125052923646318332191217321
464134655845254917228378772756695589
845219962202945089226966507426526912
7802446416400\9025927104004338958261
1419862375878988193612187945591802864
062679\864839578139273043684955597764
13009721221824915810964579376354556\6
554629883777859568089157882151127357
4220422646379170599917677567\30420698
422392494816906777896174923072071297
603455802621072109220\54662739697748
553543758990879608882627763290293452
560094576029847\3913613887675543866
22479265299978059886472414530462194
52761811989\9746477252908878060493
17954195146382922889045577804592943
73052654\10485180264002079415193983
85114342508427311982036827478946058
7100\304977477069244278989689910572
12096357725203480402449913844583448

$b =$

655456209464694; 93360682685816031704
969423104727624468251177438749706128
879957701\93698826859762790479113062
308975863428283798589097017957365590
672\83571386389571224667609499300898
554802446403039544300748002507962036
386619315229886063541005322448463915
89798641210273772558373965\486539312
854838650709031919742048649235894391
90352993032676961005\088404319792729
916038927477470940948581926791161465
02863521484987\086232861934222391717
121545686125300672760188085915004248
49476686\706784051068715397706852664
532638332403983747338379697022624261
377163163204493828299206039808703403
575100467337085017748387148822224875
309641791879395483731754620034884930
540399950519191679471224\05558557093
219350747155777569598163700850920394
705281936392411084\43600686183528465
724969562186437214972625833222544865
996160464558\54629937016589470425264
445624157899586972652935647856967092
689604\42796501209877036845001246792
761563917639959736383038665362727158

$g^{ab} =$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739
419999231378970715307039317876258453876701124543849520979430233302777503265010724513551209279573183234934359636696506
968325769489511028943698821518689496597758218540767517885836464160289471651364552490713961456608536013301649753975875
610659655755567474438180357958360226708742348175045563437075840969230826767034061119437657466993989389348289599600338
950372251336932673571743428823026014699232071116171392219599691096846714133643382745709376112500514300983651201961186
613464267685926563624589817259637248558104903657371981684417053993082671827345252841433337325420088380059232089174946
086536664984836041334031650438692639106287627157575758383128971053401037407031731509582807639509448704617983930135028
7596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468

Diffie-Hellman key exchange (cont.)

- Individual secret keys secure under Discrete Log Problem (DLP): $g, g^x \mapsto x$
- Shared secret secure under Diffie-Hellman Problem (DHP): $g, g^a, g^b \mapsto g^{ab}$
- Fundamental operation in DH is group exponentiation: $g, x \mapsto g^x$
  … done via "square-and-multiply", e.g., $(x)_2 = (1,0,1,1,0,0,0,1 \ldots)$
- We are working "$\mathbf{mod}\ q$", but only with <u>one operation</u>: multiplication
- Main reason for fields being so big: (sub-exponential) index calculus attacks!

DH key exchange (Koblitz-Miller style)

If all we need is a group, why not use elliptic curve groups?

MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 203–209

Elliptic Curve Cryptosystems

By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems may be more secure, because the analog of the discrete logarithm problem on elliptic curves is likely to be harder than the classical discrete logarithm problem, especially over $GF(2^n)$. We discuss the question of primitive points on an elliptic curve modulo p, and give a theorem on nonsmoothness of the order of the cyclic subgroup generated by a global point.

1. Introduction. The earliest public key cryptosystems using number theory were based on the structure either of the multiplicative group $(\mathbf{Z}/N\mathbf{Z})^*$ or the multiplicative group of a finite field $GF(q)$, $q = p^n$. The subsequent construction of analogous systems based on other finite Abelian groups, together with H. W. Lenstra's success in using elliptic curves for integer factorization, make it natural to study the possibility of public key cryptography based on the structure of the group of points of an elliptic curve over a large finite field. We first briefly recall the facts we need about such elliptic curves (for more details, see [4] or [5]). We then describe elliptic curve analogs of the Massey-Omura and ElGamal systems. We give some concrete examples, discuss the question of primitive points, and conclude with a theorem concerning the probability that the order of a cyclic subgroup is nonsmooth.

I would like to thank A. Odlyzko for valuable discussions and correspondence, and for sending me a preprint by V. S. Miller, who independently arrived at some similar ideas about elliptic curves and cryptography.

2. Elliptic Curves. An elliptic curve E_K defined over a field K of characteristic $\neq 2$ or 3 is the set of solutions $(x, y) \in K^2$ to the equation

$$y^2 = x^3 + ax + b, \qquad a, b \in K \tag{1}$$

(where the cubic on the right has no multiple roots). More precisely, it is the set of such solutions together with a "point at infinity" (with homogeneous coordinates $(0, 1, 0)$; if K is the real numbers, this corresponds to the vertical direction which the tangent line to E_K approaches as $x \to \infty$). One can start out with a more complicated general formula for E_K which can easily be reduced to (1) by a linear change of variables whenever $\operatorname{char} K \neq 2, 3$. If $\operatorname{char} K = 2$—an important case in

Received October 29, 1985; revised June 5, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T71, 94A60; Secondary 68P25, 11Y11, 11Y40.

203

Use of Elliptic Curves in Cryptography

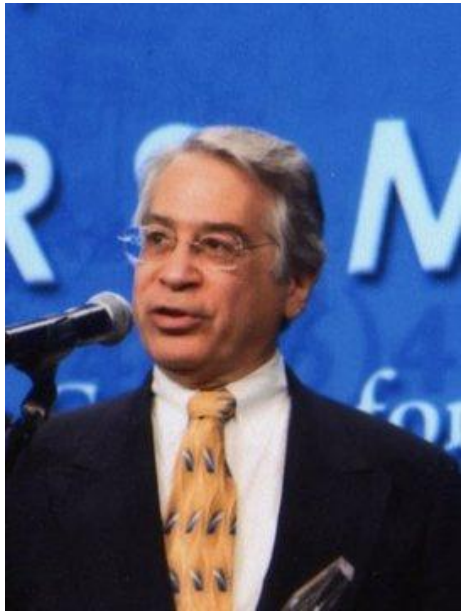
Victor S. Miller

Exploratory Computer Science, IBM Research, P.O. Box 218, Yorktown Heights, NY 10598

ABSTRACT

We discuss the use of elliptic curves in cryptography. In particular, we propose an analogue of the Diffie-Hellmann key exchange protocol which appears to be immune from attacks of the style of Western, Miller, and Adleman. With the current bounds for infeasible attack, it appears to be about 20% faster than the Diffie-Hellmann scheme over GF(p). As computational power grows, this disparity should get rapidly bigger.

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 417-426, 1986.



Rationale: "it is extremely unlikely that an index calculus attack on the elliptic curve method will ever be able to work" [Miller, 85]

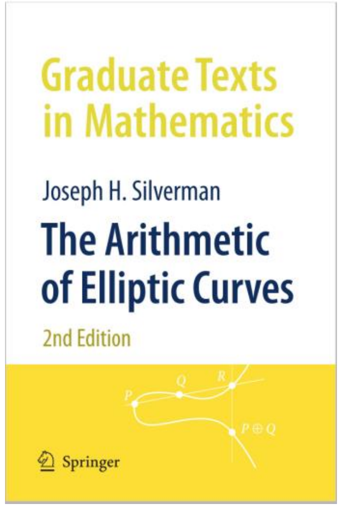
Part 1: Motivation

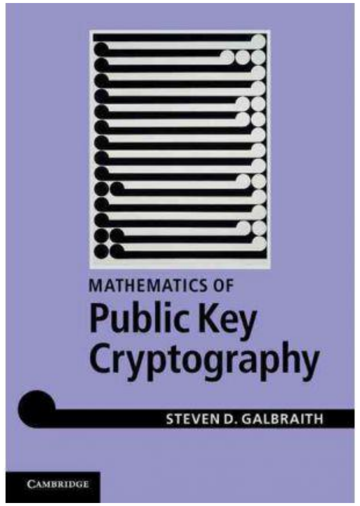
Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next-generation ECC

Some good references





Elliptic curves	Silverman's talk: "An Introduction to the Theory of Elliptic Curves" http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf

Elliptic curves	Sutherland's MIT course on elliptic curves: https://math.mit.edu/classes/18.783/2015/lectures.html

ECC	Koblitz-Menezes: ECC: the serpentine course of a paradigm shift http://eprint.iacr.org/2008/390.pdf

group	$(G, +)$	can do $+ \ -$
ring	$(R, +, \times)$	can do $+ \ - \ \times$
field	$(F, +, \times)$	can do $+ \ - \ \times \ \div$

If you've never seen an elliptic curve before….

Remember: an elliptic curve is a group defined over a field

elliptic curve group	$(\boldsymbol{E}, \oplus)$	can do $\oplus$ $\ominus$
underlying field	$(\boldsymbol{K}, +, \times)$	can do $+$ $-$ $\times$ $\div$

operations in underlying field are used and combined to compute the elliptic curve operation $\oplus$

Boring curves

$$f(x,y)=0 \qquad \text{or} \qquad f(X,Y,Z)=0$$

Degree 1 (lines)

$$ax+by=c \qquad ab\neq 0$$

Degree 2 (conic sections)

$$ax^2+bxy+cy^2+dx+ey+f=0 \qquad abc\neq 0$$

e.g., ellipses, hyperbolas, parabolas

- “Genus” measures geometric complexity, and both are genus 0
- We know how to describe all solutions to these, e.g., over (exts of) $\mathbb{Q}$
- Not cryptographically interesting

Elliptic curves

- Degree 3 is where all the fun begins…

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

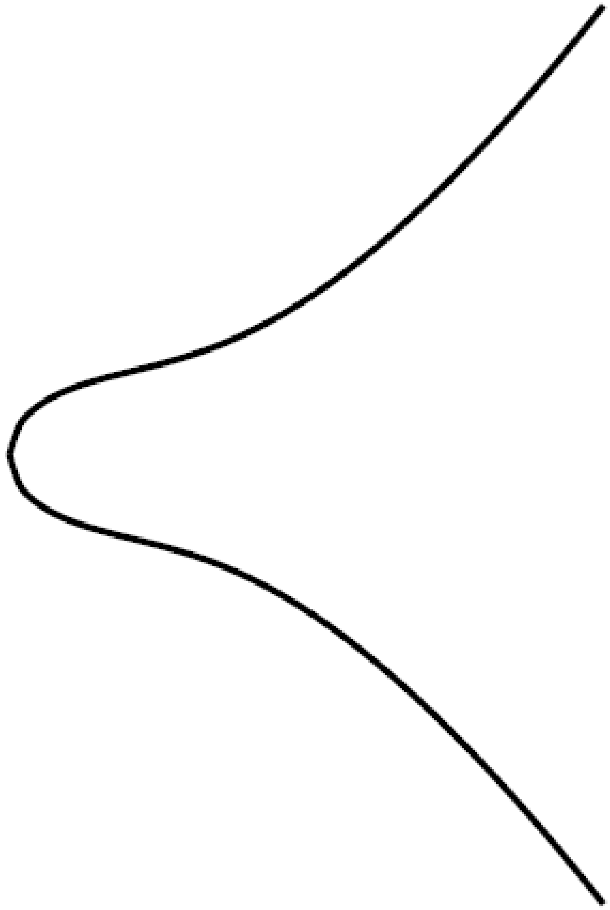
$$\Big\Downarrow \quad ch(K) \neq 2,3$$

$$E/K: \quad y^2 = x^3 + ax + b$$

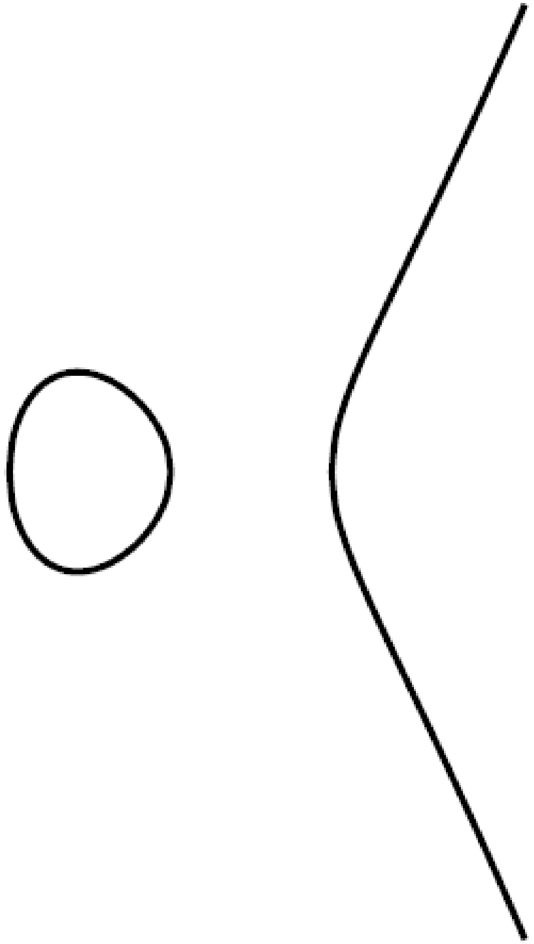
⬅ E specified by K, a, b

- Elliptic curves ↔ genus 1 curves
- Set is ≈ points $(x, y) \in K \times K$ satisfying above equation
- Geometrically/arithmetically/cryptographically interesting
- Fermat's last theorem/BSD conjecture/ …

Elliptic curves, pictorially



$E/\mathbb{R}:\ y^2 = x^3 + x + 1$



$E/\mathbb{R}:\ y^2 = x^3 - x$

Elliptic curves are groups

- So $\boldsymbol{E}$ is a set, but to be a group we need an *operation*
- The operation is between points $(x_P, y_P) \oplus (x_Q, y_Q) = (x_R, y_R)$
- Remember: a group $(E, \oplus)$ defined over a field $(K, +, \times)$
- K will be fields we're used to, e.g., $\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbb{F}_p$
- Remember: the (boring) operations $+, -, \times, \div$ in K are used to compute the (exotic) operation $\oplus$ on E

Elliptic curve group law is easy

Fun fact: homomorphism between Jacobian of elliptic curve and elliptic curve itself.

Upshot: you don't have to know what a Jacobian is to understand/do elliptic curve cryptography

The elliptic curve group law $\oplus$

We need $(x_P, y_P) \oplus (x_Q, y_Q) = (x_R, y_R)$

Question: Given two points lying on a cubic curve, how can we use their coordinates to give a third point lying on the curve?

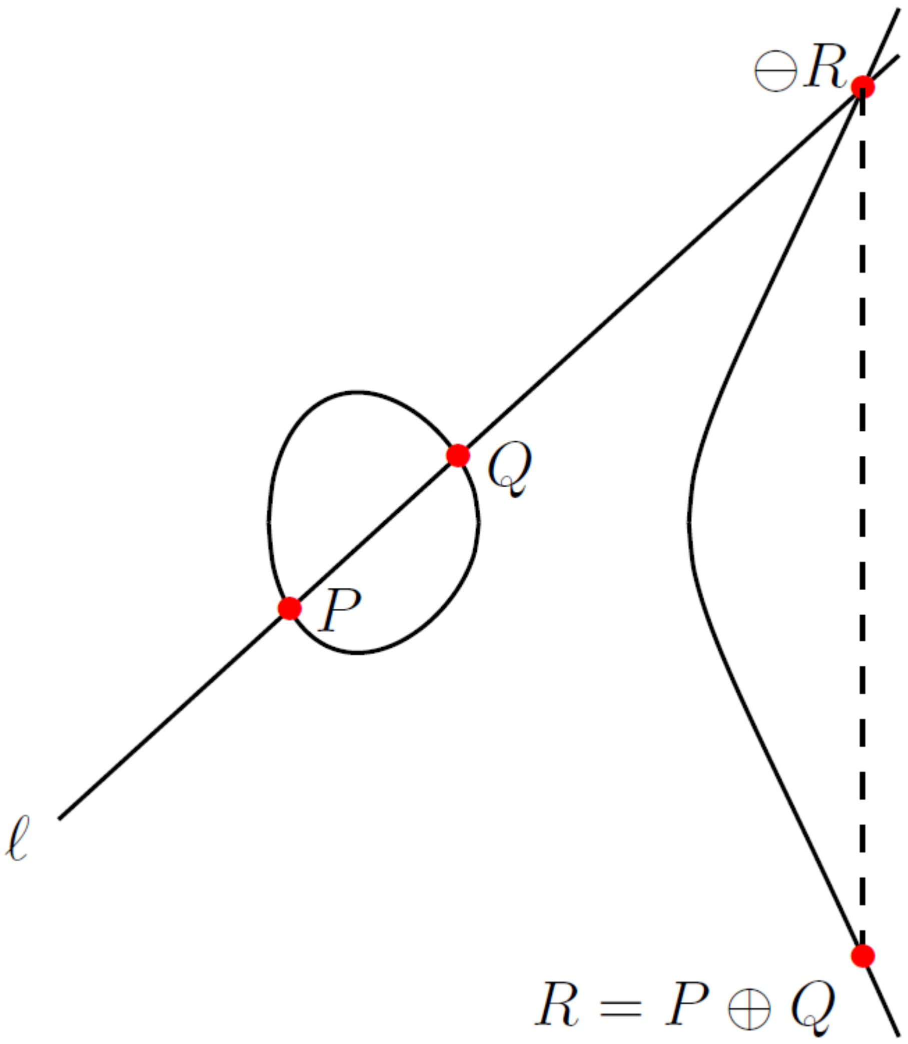
The elliptic curve group law $\oplus$

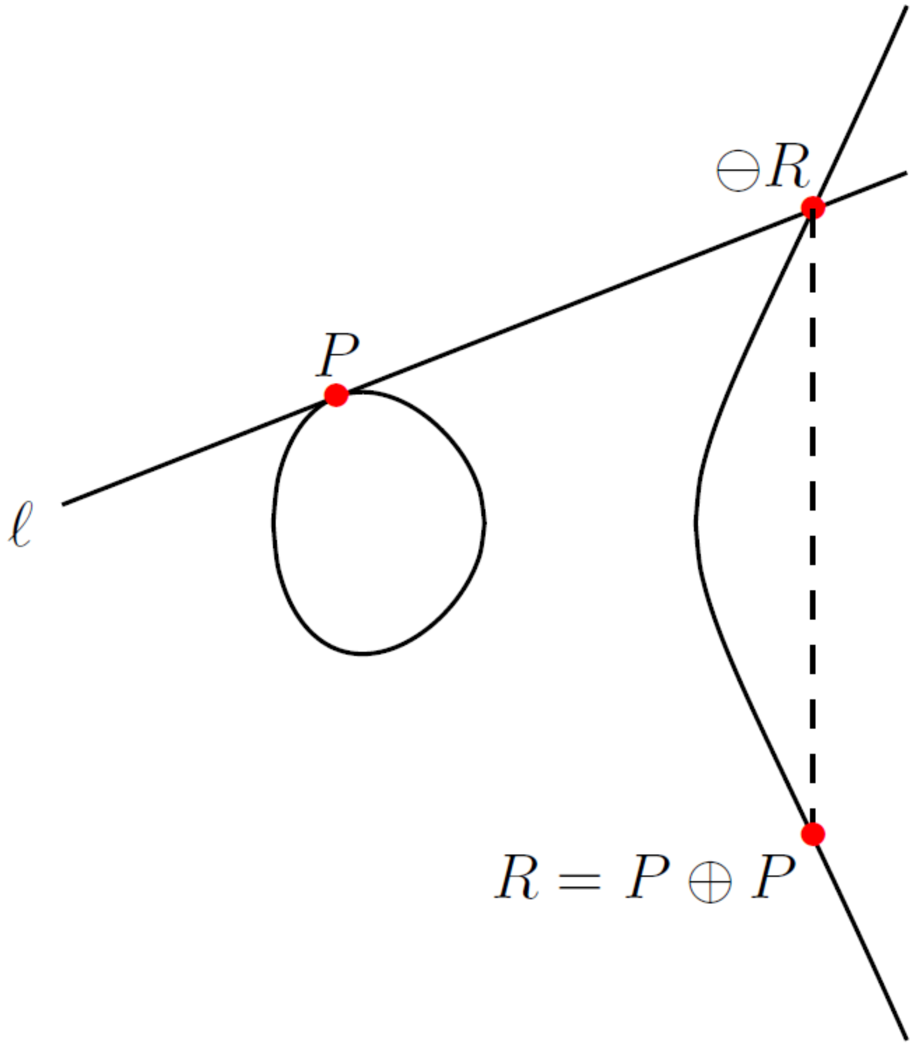
We need $(x_P, y_P) \oplus (x_Q, y_Q) = (x_R, y_R)$

Question: Given two points lying on a cubic curve, how can we use their coordinates to give a third point lying on the curve?

Answer: A line that intersects a cubic twice must intersect it again, so we draw a line through the points (x_P, y_P) and (x_Q, y_Q)

The elliptic curve group law $\oplus$



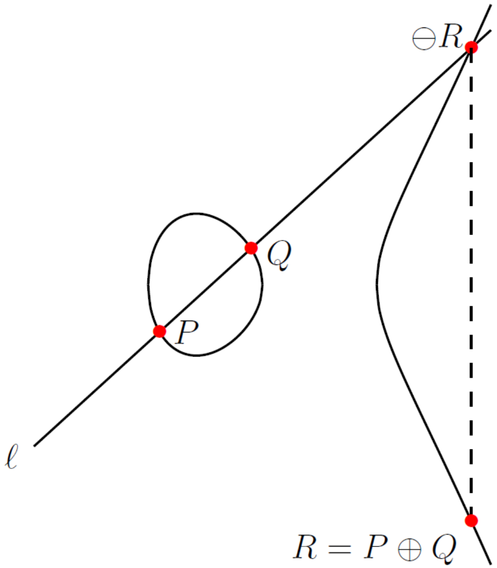


The elliptic curve group law $\oplus$

$y = \lambda x + \nu$ intersected with $y^2 = x^3 + ax + b$

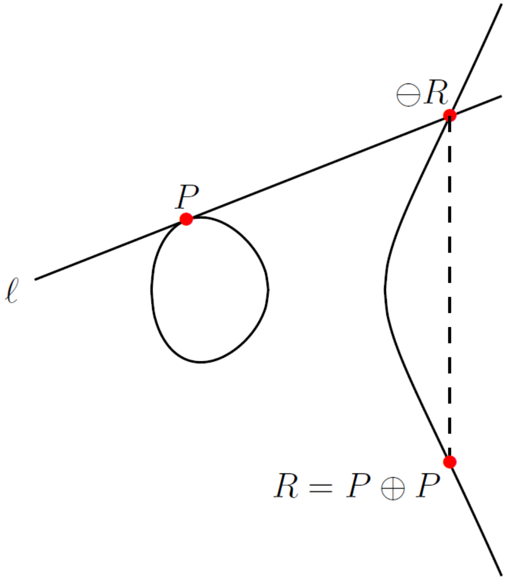
$$x^3 - (\lambda x + \nu)^2 + ax + b = 0$$

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + (b - \nu^2) = (x - x_P)(x - x_Q)(x - \boldsymbol{x_R})$$



$$x_R = \lambda^2 - x_P - x_Q$$

$$y_R = -(\lambda x_R + \nu)$$

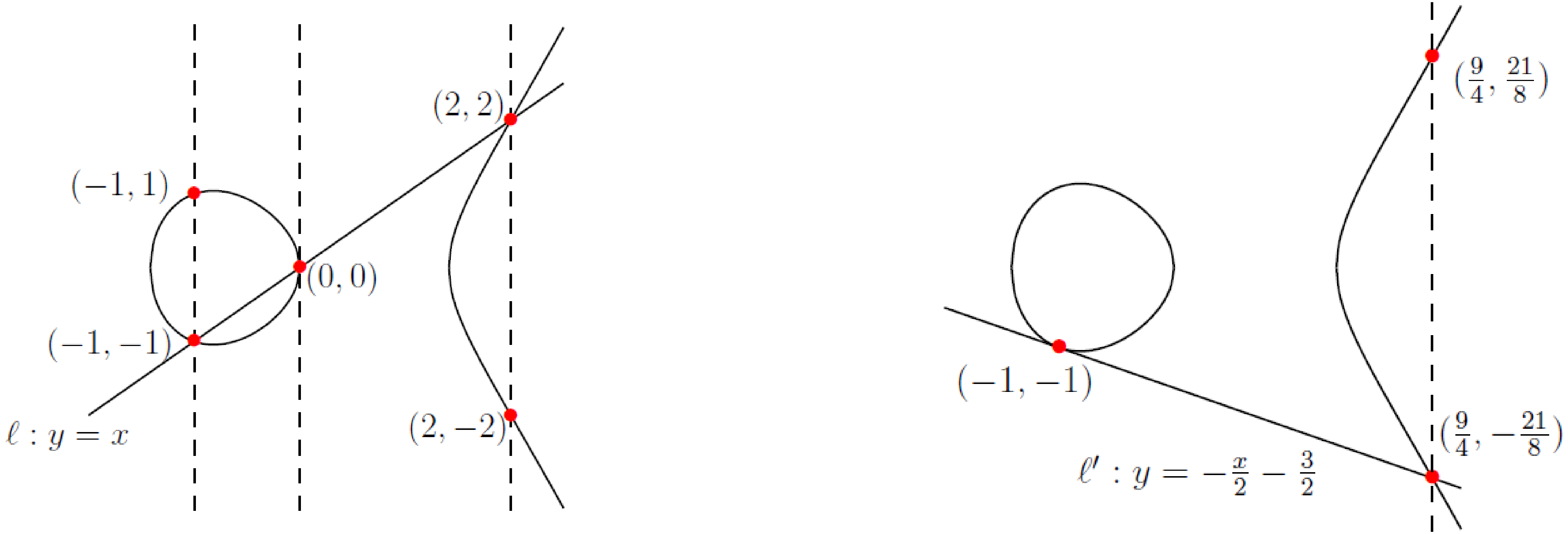


$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$\lambda = \frac{dy}{dx} = \frac{3x_P^2 + a}{2y_P}$$

A toy example

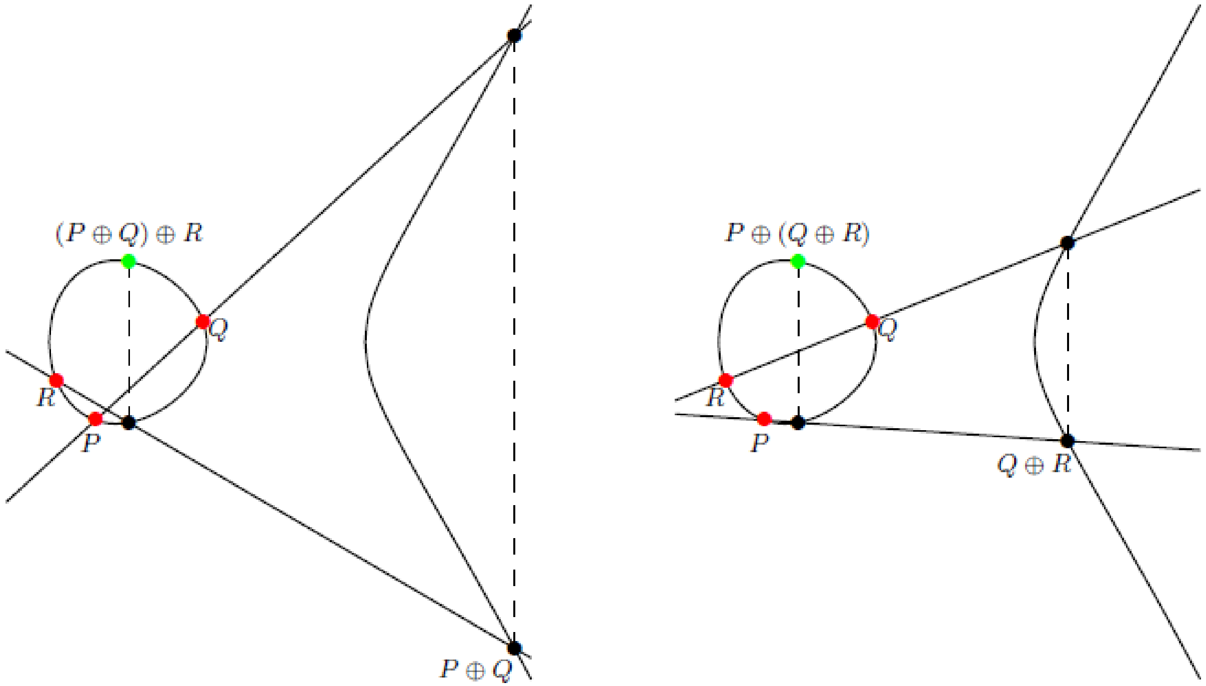
$$E/\mathbb{R}: y^2 = x^3 - 2x$$



What about $E/\mathbb{Q}: y^2 = x^3 - 2$?

The (abelian) group axioms

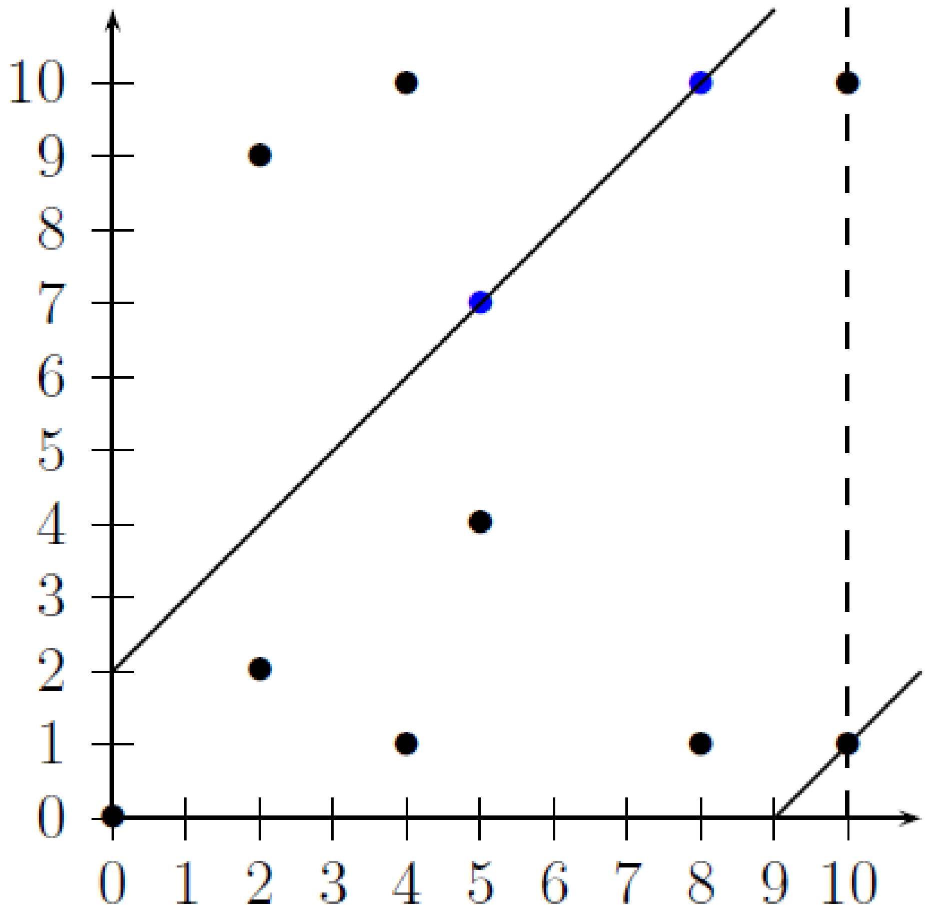
- **Closure**: the third point of intersection must be in the field
- **Identity**: $E_{a,b}(K) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{\infty\}$
- **Inverse**: $\ominus (x, y) = (x, -y)$
- **Associative**: proof by picture



- **Commutative**: line through P and Q same as line through Q and P

A toy example, cont.

$$E/\mathbb{F}_{11}: y^2 = x^3 - 2x$$



$$\#E = 12$$

$$(5,7) \oplus (8,10) = (10,10)$$

Part 1: Motivation

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next-generation ECC

Diffie-Hellman key exchange (circa 2016)

$q =$

58096059953699580628595025333045743706869751763628952366614861522872037309971102257373360445331184072513261577549805174439905295945400471216628856721870324010321116397
06440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580
16186020024749256844815024251530444957718760413642873858099017255157393414625583036640591500086964373205321856683254529110790372283163413859958640669032595972518744716
90595408050123102096390117507487600170953607342349457574162729948560133086169585299583046776370191815940885283450612858638982717634572948835466388795543116154464463301
99254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710
716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$g = 123456789$

$g^a \pmod q =$

197496648183227193286262018614250555971909799762533760654008147994875775445667054218578105133138217497206890599554928429450667899476
854668595594034093493637562451078938296960313488696178848142491351687253054602202966247046105770771577248321682117174246128321195678
537631520278649403464797353691996736993577092687178385602298873558954121056430522899619761453727082217823475746223803790014235051396
799049446508224661850168149957401474638456716624401906701394472447015052569417746372185093302535739383791980070572381421729029651639
304234361268764971707763484300668923972868709121665568669830978657804740157916611563508569886847487772676671207386096152947607114559
706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532
6052422101474898256696660124195726100495725510022002932814218768060112310763455404567248761396399633344901857872119208518550803791724

$g^b \pmod q =$

411604662069593306683228525653441872410777999220572079993574397237156368762038378332742471939666544968793817819321495269833613169937
986164811320795616949957400518206385310292475529284550626247132930124027703140131220968771142788394846592816111078275196955258045178
705254016469773509936925361994895894163065551105161929613139219782198757542984826465893457768888915561514505048091856159412977576049
073563225572809880970058396501719665853110101308432647427786556525121328772587167842037624190143909787938665842005691911997396726455
110758448552553744288464337906540312125397571803103278271979007681841394534114315726120595749993896347981789310754194864577435905673
172970033596584445206671223874399576560291954856168126236657381519414592942037018351232440467191228145585909045861278091800166330876
4073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$a =$

7147687166405;9571879053605547396582
692405186145916522354912615715297097
100679170037904924330116019497881089
087696131592831386326210951294944584
4004974889298038584931918128447572321
023987160439062006177648318875457556
2337708539125052923646318332191217321
464134655845254917228378772756695589
845219962202945089226966507426526912
7802446416400\9025927104004338958261
1419862375878988193612187945591802864
062679\864839578139273043684955597764
130097212221824915810964579376354556\6
554629883777859568089157882151127357
4220422646379170599917677567\30420698
422392494816906777896174923072071297
603455802621072109220\54662739697748
553543758990879608882627763290293452
560094576029847\3913613887675543866
22479265299978059886472414530462194
52761811989\9746477252908878060493
17954195146382922889045577804592943
73052654\10485180264002079415193983
85114342508427311982036827478946058
7100\304977477069244278989689910572
12096357725203480402449913844583448

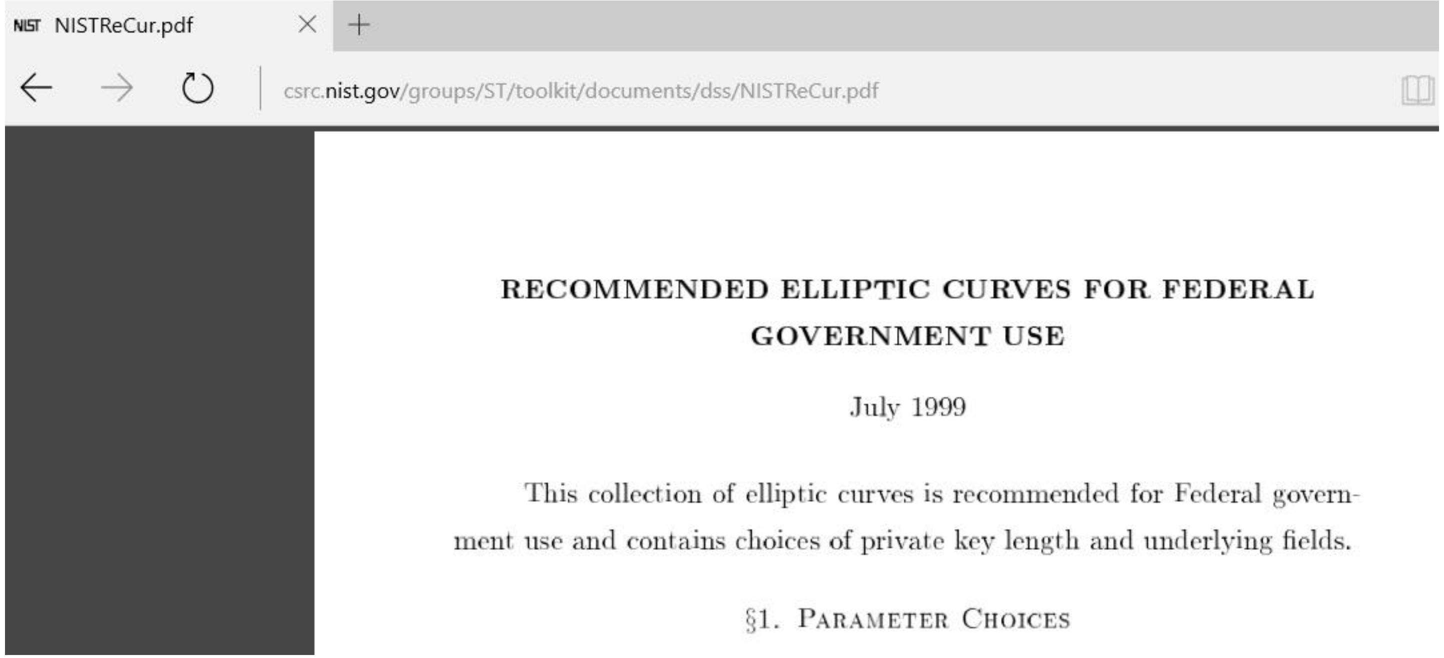
$b =$

655456209464694;93360682685816031704
969423104727624468251177438749706128
879957701\93698826859762790479113062
308975863428283798589097017957365590
672\83571386389571224667609499300898
554802446403039544300748002507962036
386619315229886063541005322448463915
89798641210273772558373965\486539312
854838650709031919742048649235894391
90352993032676961005\088404319792729
916038927477470940948581926791161465
02863521484987\086232861934222391717
121545686125300672760188085915004248
49476686\706784051068715397706852664
532638332403983747338379697022624261
377163163204493828299206039808703403
575100467337085017748387148822224875
309641791879395483731754620034884930
540399950519191679471224\05558557093
219350747155777569598163700850920394
705281936392411084\43600686183528465
724969562186437214972625833222544865
996160464558\54629937016589470425264
445624157899586972652935647856967092
689604\42796501209877036845001246792
761563917639959736383038665362727158

$g^{ab} =$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739
419999231378970715307039317876258453876701124543849520979430233302777503265010724513551209279573183234934359636696506
968325769489511028943698821518689496597758218540767517885836464160289471651364552490713961456608536013301649753975875
610659655755567474438180357958360226708742348175045563437075840969230826767034061119437657466993989389348289599600338
950372251336932673571743428823026014699232071116171392219599691096846714133643382745709376112500514300983651201961186
613464267685926563624589817259637248558104903657371981684417053993082671827345252841433337325420088380059232089174946
086536664984836041334031650438692639106287627157575758383128971053401037407031731509582807639509448704617983930135028
7596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468

NIST Curve P-256



RECOMMENDED ELLIPTIC CURVES FOR FEDERAL GOVERNMENT USE

July 1999

This collection of elliptic curves is recommended for Federal government use and contains choices of private key length and underlying fields.

§1. Parameter Choices

§2. Curves over Prime Fields

For each prime p, a pseudo-random curve

$$E: \quad y^2 \equiv x^3 - 3x + b \pmod{p}$$

Curve P-256

$p =$ 115792089210356248762697446949407573530086143415290314195533631308867097853951

$r =$ 115792089210356248762697446949407573529996955224135760342422259061068512044369

$s =$ c49d3608 86e70493 6a6678e1 139d26b7 819f7e90

$c =$ 7efba166 2985be94 03cb055c 75d4f7e0 ce8d84a9 c5114abc af317768 0104fa0d

$b =$ 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b

$G_x =$ 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296

$G_y =$ 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5

National Institute of Standards and Technology

ECDH key exchange (1999 – nowish)

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

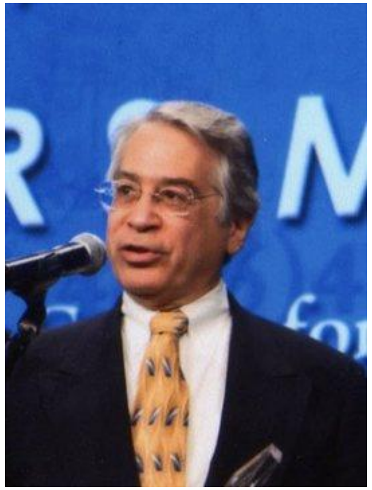
$$E/\mathbb{F}_p : y^2 = x^3 - 3x + b$$

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,$
$36134250956749795798585127919587881956611106672985015071877198253568414405109)$

$[a]P = (84116208261315898167593067868200525612344221886333785331584793435449501658416,$
$102885655542185598026739250172885300109680266058548048621945393128043427650740)$

$[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,$
$77887418190304022994116595034556257760807185615679689372138134363978498341594)$



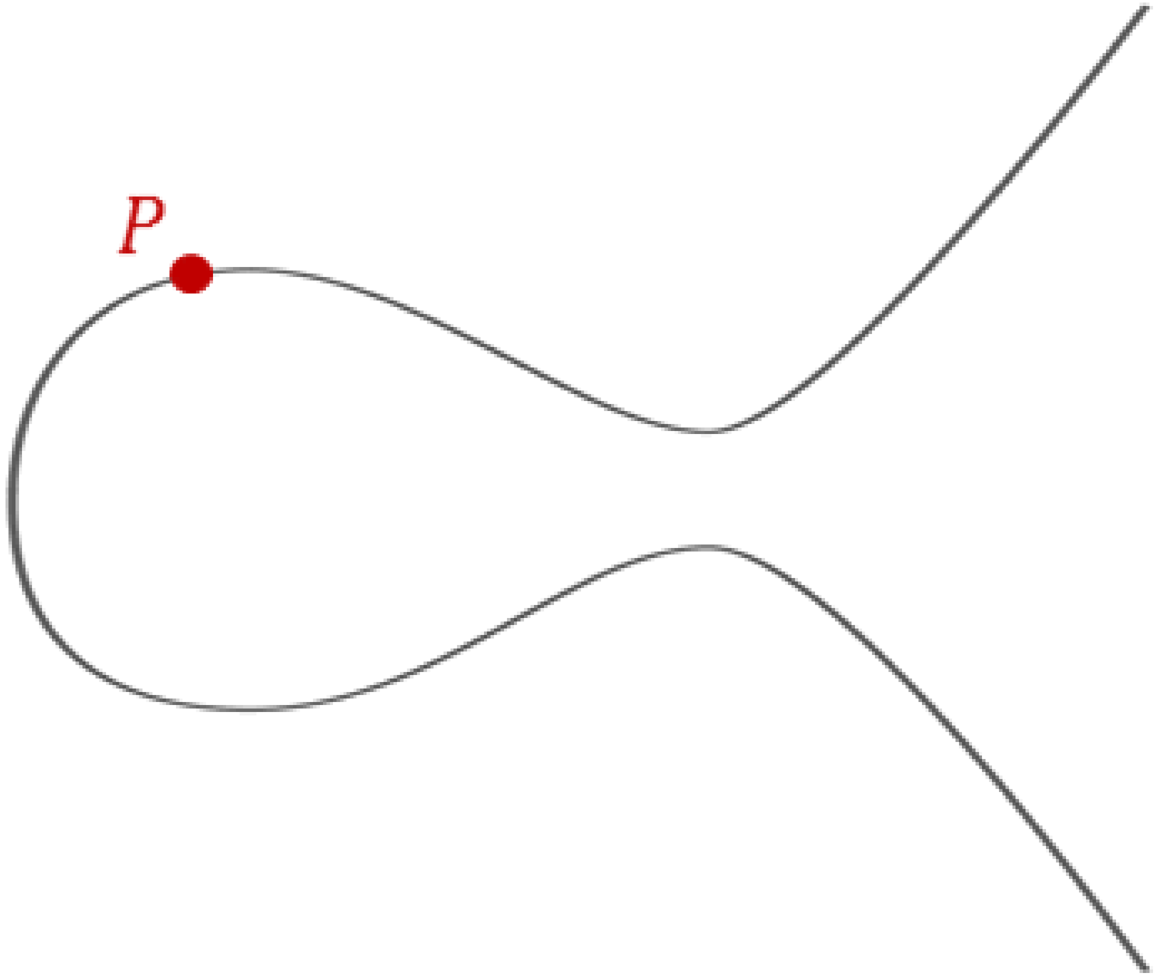
$a =$
89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

$[ab]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,$
$77887418190304022994116595034556257760807185615679689372138134363978498341594)$

$b =$
10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

The fundamental ECC operation

$$P, k \mapsto [k]P$$



GIF: Wouter Castryck

Scalar multiplications via double-and-add

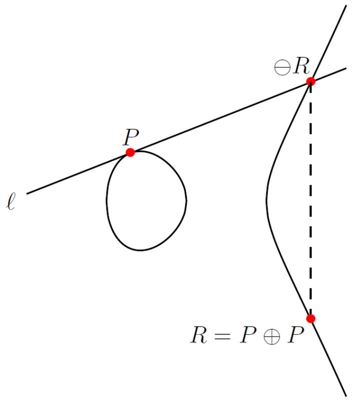
How to (naively) compute $\boldsymbol{k}, \boldsymbol{Q} \mapsto [\boldsymbol{k}]\boldsymbol{Q}$?

$P \leftarrow Q$

$k = (k_n, k_{n-1}, \ldots, k_0)_2$

for i from $n-1$ downto 0 do

$P \leftarrow [2]P$

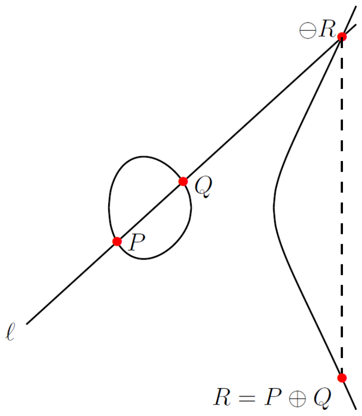


DBL

if $k_i = 1$ then

$P \leftarrow P \oplus Q$

end if



ADD

end for

return $P\ (= [k]Q)$

Scalar multiplications via double-and-add

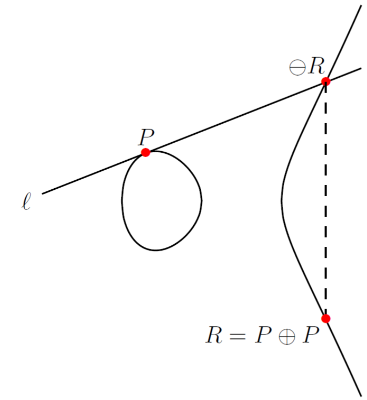
How to (naively) compute $\boldsymbol{k, Q} \mapsto [\boldsymbol{k}]\boldsymbol{Q}$?

$$P \leftarrow Q$$

$$k = (k_n, k_{n-1}, \dots, k_0)_2$$

for i from $n-1$ downto 0 do

$$P \leftarrow [2]P$$

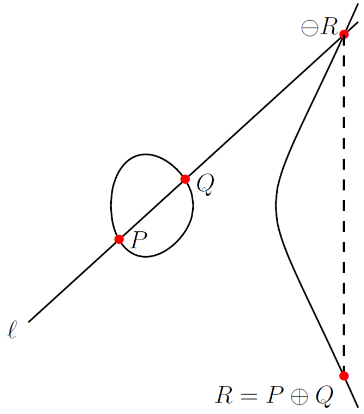


DBL

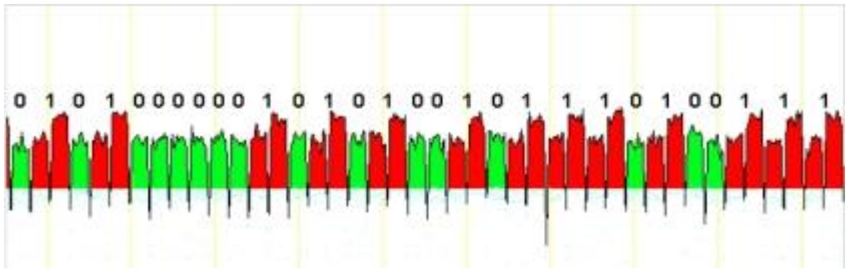
if $k_i = 1$ then

$$P \leftarrow P \oplus Q$$

end if



ADD



end for

return $P\ (= [k]Q)$

Scalar multiplications via double-and-add

How to compute $k, Q \mapsto [k]Q$ on $y^2 = x^3 + ax + b$?

$$k = (k_n, k_{n-1}, \dots, k_0)$$

$$(x_P, y_P) \leftarrow Q$$

for i from $n-1$ downto 0 do

$$\lambda \leftarrow (3x_P^2 + a)/(2y_P)\,; \qquad \nu \leftarrow y_P - \lambda x_P\,;$$

$$x_P \leftarrow \lambda^2 - 2x_P; \qquad y_P \leftarrow -(\lambda x_P + \nu);$$

if $k_i = 1$ then

$$\lambda \leftarrow (y_P - y_Q)/(x_P - x_Q)\,; \quad \nu \leftarrow y_P - \lambda x_P\,;$$

$$x_P \leftarrow \lambda^2 - x_P - x_Q; \quad y_P \leftarrow -(\lambda x_P + \nu)$$

end for

return $(x_P, y_P) = [k](x_Q, y_Q)$

Projective space

- Recall we defined the group of K-rational points as
$$E_{a,b}(K) = \{(x,y): y^2 = x^3 + ax + b\} \cup \{\infty\}$$

- The *natural habitat* for elliptic curve groups is in $\mathbb{P}^2(K)$, not $\mathbb{A}^2(K)$

- For (easiest) example, rather than $(x,y) \in \mathbb{A}^2$, take $(X:Y:Z) \in \mathbb{P}^2$ modulo the equivalence $(X:Y:Z) \sim (\lambda X : \lambda Y : \lambda Z)$ for $\lambda \in K^*$

- Replace x with X/Z and y with Y/Z, so $E_{a,b}(K)$ is the set of solutions $(X:Y:Z) \in \mathbb{P}^2(K)$ to
$$E : \quad Y^2Z = X^3 + aXZ^2 + bZ^3$$

- So the affine points (x,y) from before become $(x : y : 1) \sim (\lambda x : \lambda y : \lambda)$ and the point at infinity is the unique point with $Z = 0$, i.e., $(0 : 1 : 0) \sim (0 : \lambda : 0)$

Projective space, cont.

- One practical benefit of working over $\mathbb{P}^2$ is that the explicit formulas for computing $\oplus$ become much faster, by avoiding field inversions

- Thus, the fundamental ECC operation $k, P \mapsto [k]P$ becomes much faster…

$(x', y') = [2](x, y)$	$(X' : Y' : Z') = [2](X : Y : Z)$
$\lambda \leftarrow (3x^2 + a)/(2y)\,;$ $x' \leftarrow \lambda^2 - 2x;$ $y' \leftarrow -(\lambda(x' - x) + y);$	$X' = 2XY\left(\left(3X^2 + aZ^2\right)^2 - 8Y^2XZ\right)$ $Y' = \left(3X^2 + aZ^2\right)\left(12Y^2XZ - \left(3X^2 + aZ^2\right)^2\right) - 8Y^4Z^2$ $Z' = 8Y^3Z^3$
$1S + 2M + 1I$	$5M + 6S$

Projective scalar multiplications

How to compute $k, Q \mapsto [k]Q$ on $y^2 = x^3 + ax + b$?

$k = (k_n, k_{n-1}, \ldots, k_0)$

$(X_P : Y_P : Z_P) \leftarrow Q$

for i from $n-1$ downto 0 do

$(X_P : Y_P : Z_P) \leftarrow [2](X_P : Y_P : Z_P)$ $5M + 6S$

if $k_i = 1$ then

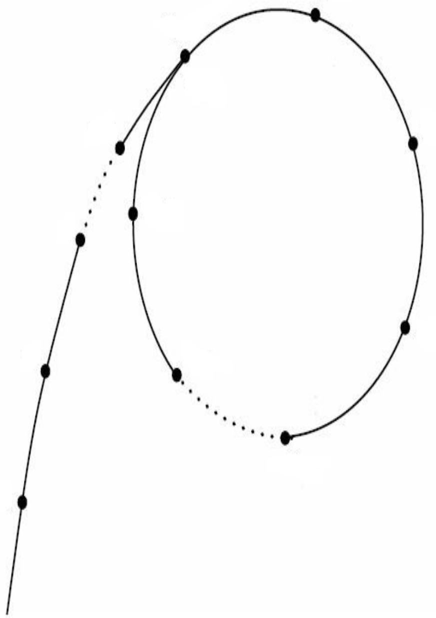
$(X_P : Y_P : Z_P) \leftarrow (X_P : Y_P : Z_P) \oplus (X_Q : Y_Q : Z_Q)$ $9M + 2S$

end for

return $(x_P, y_P) \leftarrow (X_P/Z_P, Y_P/Z_P)$ $1I + 2M$

ECDLP security and Pollard's rho algorithm

- ECDLP: given $P, Q \in E(\mathbb{F}_p)$ of prime order N, find k such that $Q = [k]P$
- Pollard'78: compute pseudo-random $R_i = [a_i]P + [b_i]Q$ until we find a collision $R_i = R_j$ with $b_i \neq b_j$, then $k = (a_j - a_i)/(b_i - b_j)$
- Birthday paradox says we can expect collision after computing $\sqrt{\pi n/2}$ group elements R_i, i.e., after $\approx \sqrt{N}$ group operations. So 2^{128} security needs $N \approx 2^{256}$
- The best known ECDLP algorithm on (well-chosen) elliptic curves remains generic, i.e., elliptic curves are as strong as is possible



Index calculus on elliptic curves?

[Miller, 85] : "it is extremely unlikely that an index calculus [...] will ever be able to work"

Consider $E/\mathbb{F}_{1217}$: $y^2 = x^3 - 3x + 139$

$\#E(\mathbb{F}_{1217}) = 1277$

$P = (3{,}401)$ and $Q = (192{,}847)$

ECDLP: find k such that $[k]P = Q$

Regardless of factor base, can't efficiently decompose elements!

e.g., factor base $R_i = \{(3{,}401), (5{,}395), (7{,}73), (11{,}252), (13{,}104), (19{,}265)\}$

Writing $S = \sum [k_i] R_i$ involves solving discrete logarithms, compare this to integers $\mathbf{mod}\ p$ where we lift and factorise over the integers

Part 1: Motivation

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next-generation ECC

What’s wrong with old school ECC?

- **Side-channel attacks**: starting with Kocher’99, side-channel attacks and their countermeasures have become extremely sophisticated
- **Decades of new research:** we now know much better/faster/simpler/safer ways to do ECC
- **Suspicion surrounding previous standards**: Snowden leaks, dual EC-DRBG backdoor, etc., lead to conjectured weaknesses in the NIST curves

Next generation elliptic curves

- 2014: CFRG receives formal request from TLS working group for recommendations for new elliptic curves
- 2015: NIST holds workshop on ECC standards
- 2015: CFRG announces two chosen curves, both specified in Montgomery (1987) form

$$E/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$$

- Bernstein's Curve25519 [2006]: $p = 2^{255} - 19$ and $A = 486662$
- Hamburg's Goldilocks [2015]: $p = 2^{448} - 2^{224} - 1$ and $A = 156326$
- Both primes offer fast software implementations!
- Their group orders are divisible by 8 and 4, but this form offers several advantages.

Montgomery's fast differential arithmetic

$$E/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$$

- drop the y-coordinate, and work with x-only.
- projectively, work with $(X : Z) \in \mathbb{P}^1$ instead of $(X : Y : Z) \in \mathbb{P}^2$
- But (pseudo-)addition of $\mathrm{x}(P)$ and $\mathrm{x}(Q)$ requires $x(Q \ominus P)$

Extremely fast pseudo-doubling: xDBL

$$X_{[2]P} = (X_P + Z_P)^2(X_P - Z_P)^2$$

$$Z_{[2]P} = 4X_PZ_P((X_P - Z_P)^2 + (A+2)X_PZ_P)$$

$2M + 2S$

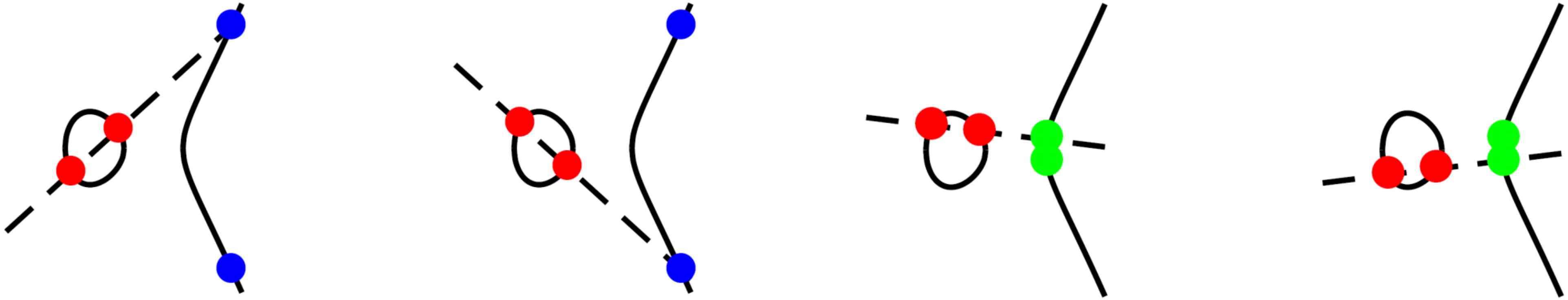
Extremely fast pseudo-addition: xADD

$$X_{P+Q} = Z_{P-Q}\left[(X_P - Z_P)(X_Q + Z_Q) + (X_P + Z_P)(X_Q - Z_Q)\right]^2$$

$$Z_{P+Q} = X_{P-Q}\left[(X_P - Z_P)(X_Q + Z_Q) - (X_P + Z_P)(X_Q - Z_Q)\right]^2$$

$4M + 2S$

Differential additions and the Montgomery ladder



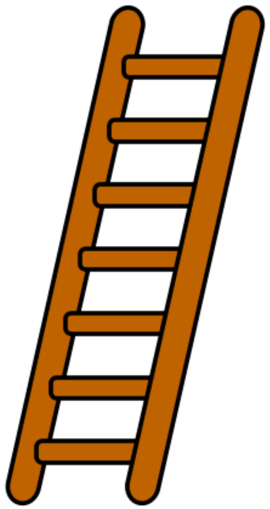
- Given only the x-coordinates of two points, the x-coordinate of their sum can be two possibilities
- Inputting the x-coordinate of the *difference* resolves ambiguity
- The (ingenious!) Montgomery ladder fixes all *differences* as the input point: in $k, x(P) \mapsto x([k]P)$, every $\mathbf{xADD}$ is of the form

$$\mathrm{xADD}(x([n+1]P), x([n]P), x(P))$$

- We carry two multiples of P "up the ladder": $x(Q)$ and $x(Q \oplus P)$
- At i^{th}step: compute $x([2]Q \oplus P) = xADD(x(Q \oplus P), x(Q), x(P))$
- At i^{th}step: pseudo-double ($\mathbf{xDBL}$) one of them depending on k_i

Fast, compact, simple, safer Diffie-Hellman

- Write $k = \sum_{i=0}^{\ell-1} k_i 2^i$ with $k_{\ell-1} = 1$ and $P = (x_P, y_P)$ in E (e.g., on Curve25519 or Goldilocks)



$(x_0, x_1) \leftarrow (\mathrm{xDBL}(x_P), x_P)$
for $i = \ell - 2$ downto 0 do
  $(x_0, x_1) \leftarrow \mathrm{cSWAP}\big((k_{i+1} \otimes k_i), (x_0, x_1)\big)$
  $(x_0, x_1) \leftarrow (\mathrm{xDBL}(x_0), \mathrm{xADD}(x_0, x_1, x_P))$
end for
$(x_0, x_1) \leftarrow \mathrm{cSWAP}\big(k_0, (x_0, x_1)\big)$
return x_0 $(= x_{[k]P})$

Inherently uniform, much easier to implement in constant-time

- x-only Diffie-Hellman (Miller'85): $x([ab]P) = x\big([a]([b]P)\big) = x([b]([a]P))$

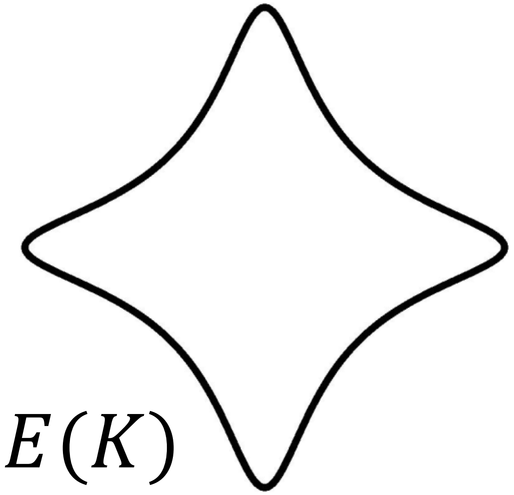
see https://tools.ietf.org/html/rfc7748

(Elliptic curves for security)

Curve25519 and Goldilocks in the real world

- See “Elliptic curves for security” https://tools.ietf.org/html/rfc7748
- Both curves integrated into TLS ciphersuites
- In 2014, OpenSSH defaults to Curve25519
- Curve25519 is used in Signal Protocol (Facebook Messenger, Google Allo, WhatsApp), iOS, GnuPG, etc (https://en.wikipedia.org/wiki/Curve25519)

(Twisted) Edwards curves



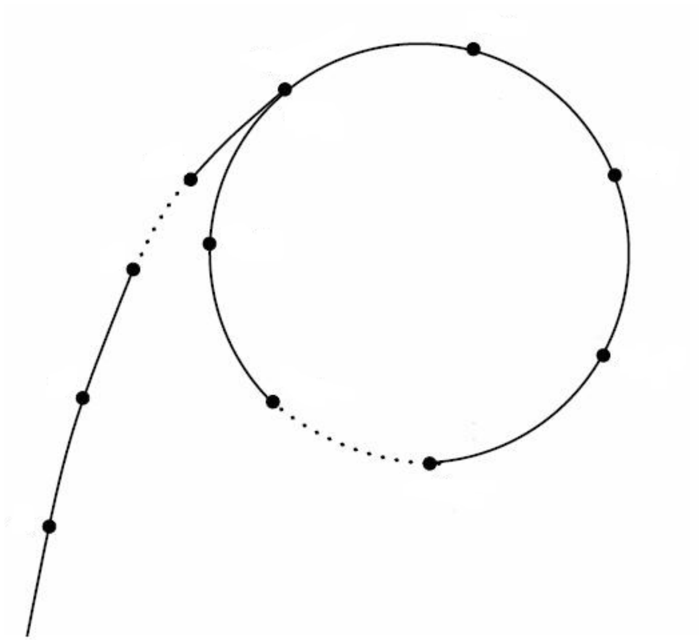
$$E : ax^2 + y^2 = 1 + dx^2y^2$$

- Neutral element is $(0,1)$ - no projective space needed for $E(K)$
- Addition law is *complete* (for well-chosen E)

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_1 + x_2y_2}{y_1y_2 - x_1x_2}, \frac{x_1y_1 - x_2y_2}{x_1y_2 - y_1x_2} \right)$$

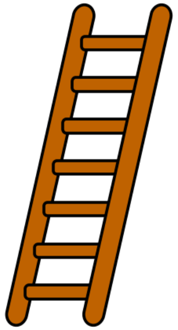
- Extremely fast: 8M! Also works for doubling, inverses, everything
- Fast, simple, exception-free implementations that always compute correctly
- Also birationally equivalent to Montgomery curves!

Elliptic curves: the best of both worlds



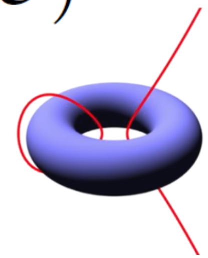
$\mathbb{P}^1 \times \mathbb{P}^1$

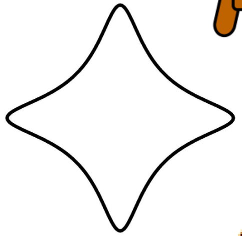
$\mathcal{L} \in \mathbb{R}^n$



$\mathrm{Hom}(\mathcal{E}, \hat{\mathcal{E}})$

ϕ





ψ

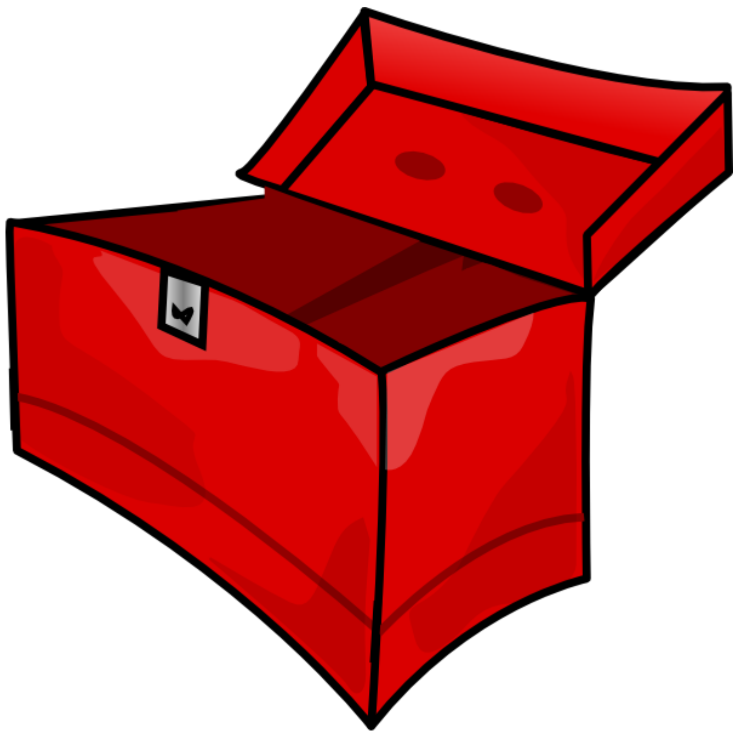
$\pi_p : \mathcal{E}_{\mathrm{W}}^{\sigma} \to \mathcal{E}_{\mathrm{W}}$

$\mathbb{Q}(\sqrt{D})$

$\tau : \mathcal{E} \to \hat{\mathcal{E}}$

attacker: generic vs. us: not generic

ECC is the best of both worlds



attacker's toolbox vs. our toolbox

Questions?