

An introduction to elliptic curve cryptography

Craig Costello

Microsoft®
Research

Part 1: Cryptography

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next talk?



MORE ACM AWARDS



Search

TYPE HERE



A.M. TURING AWARD WINNERS BY...

ALPHABETICAL LISTING

YEAR OF THE AWARD

RESEARCH SUBJECT



2015 AWARD WINNERS:

**Whitfield Diffie and
Martin Hellman**

Cryptography Pioneers Receive 2015 ACM A.M. Turing Award

Whitfield Diffie, former Chief Security Officer of Sun Microsystems and **Martin E. Hellman**, Professor Emeritus of Electrical Engineering at Stanford University, are the recipients of the 2015 ACM A.M. Turing Award, for critical contributions to modern cryptography. The ability for two parties to communicate privately over a secure channel is fundamental for billions of people around the world. On a daily basis, individuals establish secure online connections with banks, e-commerce sites, email servers and the cloud. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography," introduced the ideas of public-key

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

1. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975, and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.

M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D . Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is a multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver's public enciphering key and decipheres the messages he receives using his own secret deciphering key.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of a different form.

A second problem, amenable to cryptographic solution, which stands in the way of replacing contemporary busi-

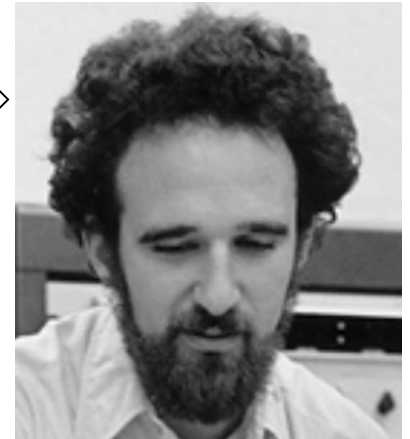
Diffie-Hellman key exchange (circa 1976)

$q = 1606938044258990275541962092341162602522202993782792835301301$

$g = 123456789$



$g^a \bmod q = 78467374529422653579754596319852702575499692980085777948593$



$560048104293218128667441021342483133802626271394299410128798 = g^b \bmod q$

$a =$

685408003627063
761059275919665
781694368639459
527871881531452

$b =$

362059131912941
987637880257325
269696682836735
524942246807440

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

Diffie-Hellman key exchange (circa 2016)

$$q =$$

5809605995369958062859502533304574370686975176362895236661486152287203730997110225737336044533118407251326157754980517443990529594540047121662885672187032401032111639706440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580161860200247492568448150242515304449577187604136428738580990172551573934146255830366405915000869643732053218566832545291107903722831634138599586406690325959725187447169059540805012310209639011750748760017095360734234945757416272994856013308616958529958304677637019181594088528345061285863898271763457294883546638879554311615446446330199254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$$g = 123456789$$

$$g^a \pmod q =$$

19749664818322719328626201861425055597190979976253376065400814799487577544566705421857810513313821749720689059955492842945066789947685466859559403409349363756245107893829696031348869617884814249135168725305460220296624704610577077157724832168211717424612832119567853763152027864940346479735369199673699357709268717838560229887355895412105643052289961976145372708221782347574622380379001423505139679904944650822466185016814995740147463845671662440190670139447244701505256941774637218509330253573938379198007057238142172902965163930423436126876497170776348430066892397286870912166556869830978657804740157916611563508569886847487772676671207386096152947607114559706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532605242210147489825669666012419572610049572551002200293281421876806011231076345540456724876139639963344901857872119208518550803791724

4116046620695933066832285256534418724107779992205720799935743972371563687620383783327424719396665449687938178193214952698336131699379861648113207956169499574005182063853102924755292845506262471329301240277031401312209687711427883948465928161110782751969552580451787052540164697735099369253619948958941630655511051619296131392197821987575429848264658934577688889155615145050480918561594129775760490735632255728098809700583965017196658531101013084326474277865655251213287725871678420376241901439097879386658420056919119973967264551107584485525537442884643379065403121253975718031032782719790076818413945341143157261205957499938963479817893107541948645774359056731729700335965844452066712238743995765602919548561681262366573815194145929420370183512324404671912281455859090458612780918001663308764073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$$= g^b \pmod q$$

$$a =$$



7147687166405; 9571879053605547396582692405186145916522354912615715297097100679170037904924330116019497881089087696131592831386326210951294944584400497488929803858493191812844757232102398716043906200617764831887545755623377085391250529236463183321912173214641346558452549172283787727566955898452199622029450892269665074265269127802446416400\97464722529088780604931419862375878988193612187945591802864062679\86483957813927304368495559776413009721221824915810964579376354556\65546298837778595680891578821511273574220422646379170599917677567\30420698422392494816906777896174923072071297603455802621072109220\5466273969774855343758990879608882627763290293452560094576029847\39136138876755438662247926529997805988647241453046219452761811989\97464722529088780604931795419514638292288904557780459294373052654\10485180264002079415193983851143425084273119820368274789460587100\30497747706924427898968991057212096357725203480402449913844583448

$$g^ab =$$

330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739419999231378970715307039317876258453876701124543849520979430233302775032650107245135512092795731832349343596366965069683257694895110289436988215186894965977582185407675178858364641602894716513645524907139614566085360133016497539758756106596557555674744381803579583602267087423481750455634370758409692308267670340611194376574669939893893482895996003389503722513369326735717434288230260146992320711161713922195996910968467141336433827457093761125005143009836512019611866134642676859265636245898172596372485581049036573719816844170539930826718273452528414333373254200883800592320891749460865366649848360413340316504386926391062876271575757583831289710534010374070317315095828076395094487046179839301350287596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468

$$b =$$



655456209464694; 93360682685816031704969423104727624468251177438749706128879957701\93698826859762790479113062308975863428283798589097017957365590672\835713863895712246676094993008985548024464030395443007480025079620363866193152298860635410053224484639158978641210273772558373965\48653931285483865070903191974204864923589439190352993032676961005\08840431979272991603892747747094094858192679116146502863521484987\08623286193422239171712154568612530067276018808591500424849476686\706784051068715397706852664532638332403983747338379697022624261377163163204493828299206039808703403575100467337085017748387148822224875309641791879395483731754620034884930540399950519191679471224\055585570932193507471557775698163700850920394705281936392411084\43600686183528465724969562186437214972625833222544865996160464558\5462993701658947042526445624157899586972652935647856967092689604\42796501209877036845001246792761563917639959736383038665362727158

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 key exchange is group exponentiation: $g, x \mapsto g^x$
Done via “square-and-multiply”, e.g., $(x)_2 = (1,0,1,1,0,0,0,1 \dots)$
- We are working “**mod** q ”, but only with one operation: multiplication
- Actually, fundamental operation in all public-key cryptography (key exchange, signatures, encryption, etc) is group exponentiation
- Main reason for fields being so big: (sub-exponential) index calculus attacks! (more later)

DH key exchange (Koblitz-Miller style)

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



MATHEMATICS OF COMPUTATION
VOLUME 49, NUMBER 177
JANUARY 1987, PAGES 203-204

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 $\text{GF}(2^n)$. 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 $(\mathbb{Z}/N\mathbb{Z})^*$ or the multiplicative group of a finite field $\text{GF}(q)$, $q = p^n$. 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

$$(1) \quad y^2 = x^3 + ax + b, \quad a, b \in K$$

(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 $x \rightarrow \infty$). 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 $\text{char } K \neq 2, 3$. If $\text{char } K = 2$ —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.

©1987 American Mathematical Society
0025-5718/87 \$1.00 + \$.25 per page

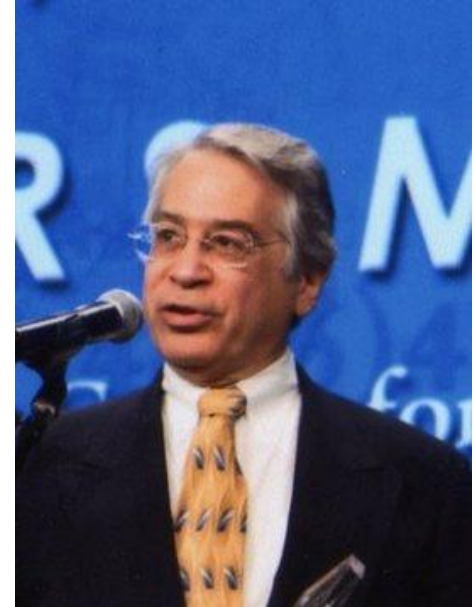
Use of Elliptic Curves in Cryptography

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 $\text{GF}(p)$. 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.
© Springer-Verlag Berlin Heidelberg 1986

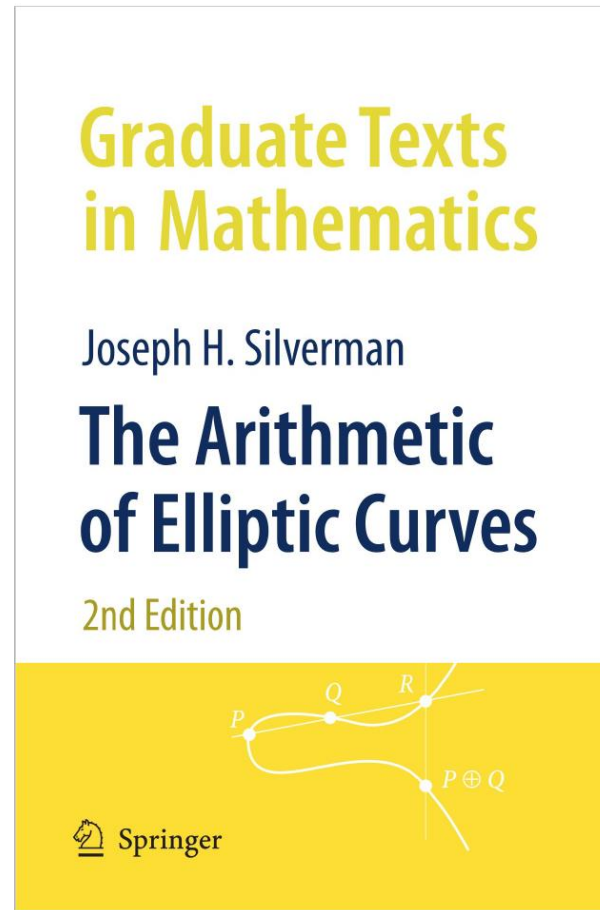
Part 1: Cryptography

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next talk?

The Bible:



or "An Introduction to the Theory of Elliptic Curves"

<http://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf>

group $(G, +)$

can do $+$ $-$

ring $(R, +, \times)$

can do $+$ $-$ \times

field $(F, +, \times)$

can do $+$ $-$ \times \div

Boring curves

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

Degree 1 (lines)

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

Degree 2 (conic sections)

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

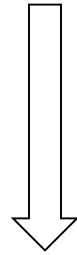
e.g., ellipses, hyperbolas, parabolas

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

Elliptic curves

- Degree 3 is where all the fun begins...

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

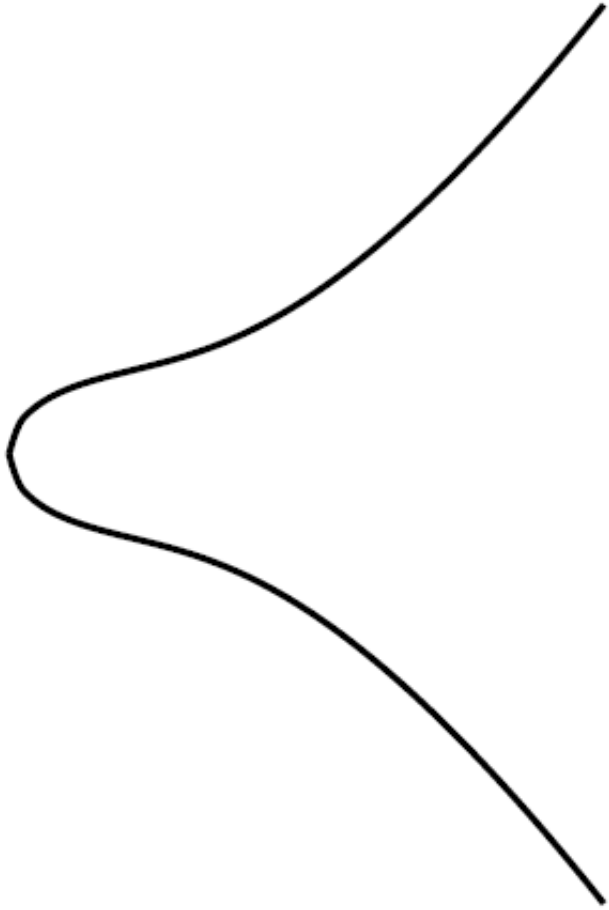


$$ch(K) \neq 2, 3$$

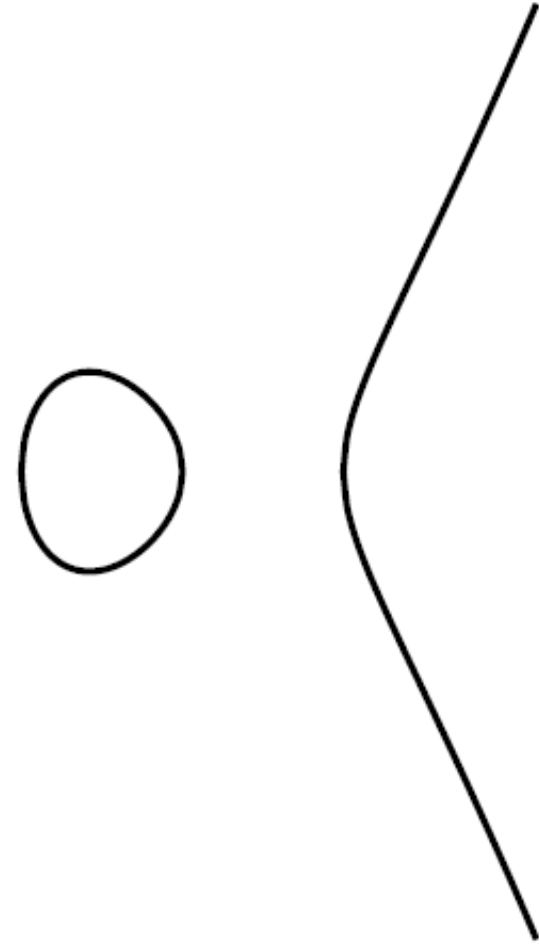
$$E/K: y^2 = x^3 + ax + b$$

- Elliptic curves \leftrightarrow genus 1 curves
- Set of 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 E is a set, but to be a group we need an *operation*
- The operation is between points $(x_P, y_P) \oplus (x_Q, y_Q) = (x_R, y_R)$
- A group (E, \oplus) defined over a field $(K, +, \times)$
- K will be fields we're used to, e.g., $\mathbb{Q}, \mathbb{C}, \mathbb{R}, \mathbf{F}_p$
- 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 any algebraic geometry (e.g., language of divisors) to understand/do elliptic curve cryptography

The elliptic curve group law \oplus

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

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

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

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)

$$y = \lambda x + \nu \quad \cap \quad y^2 = x^3 + ax + b$$

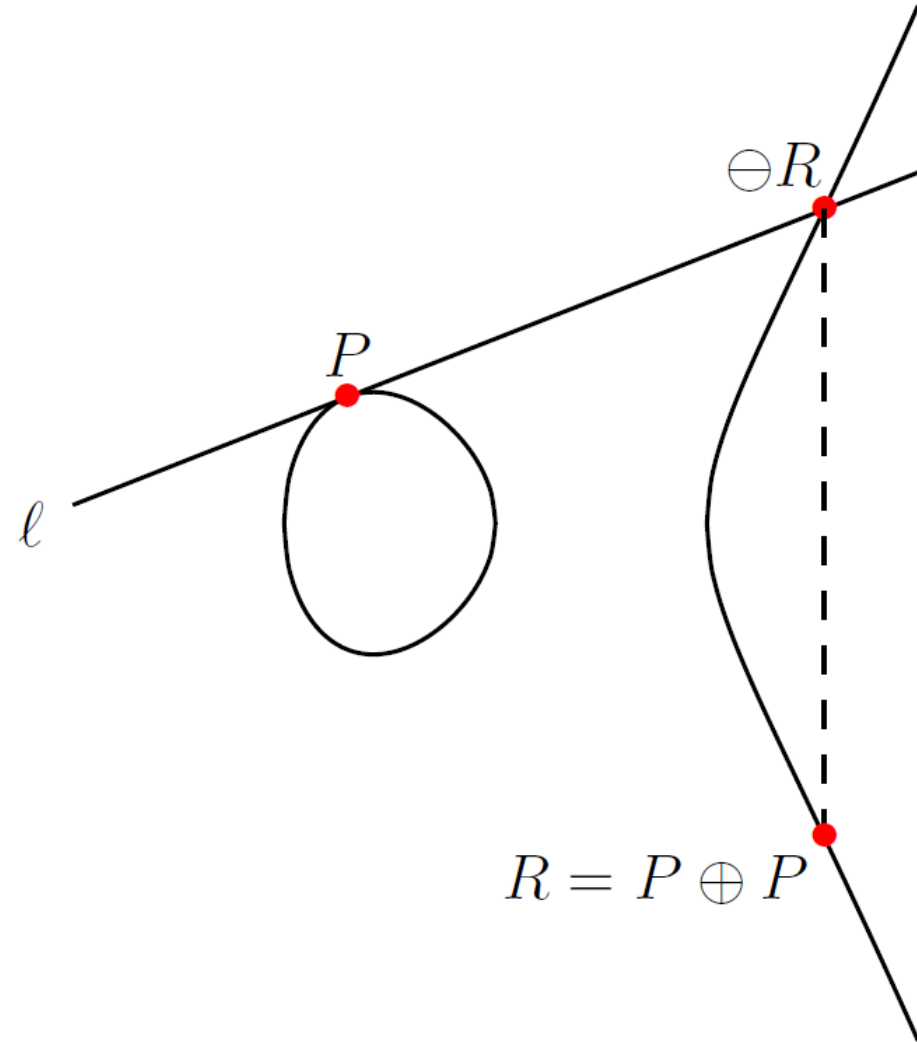
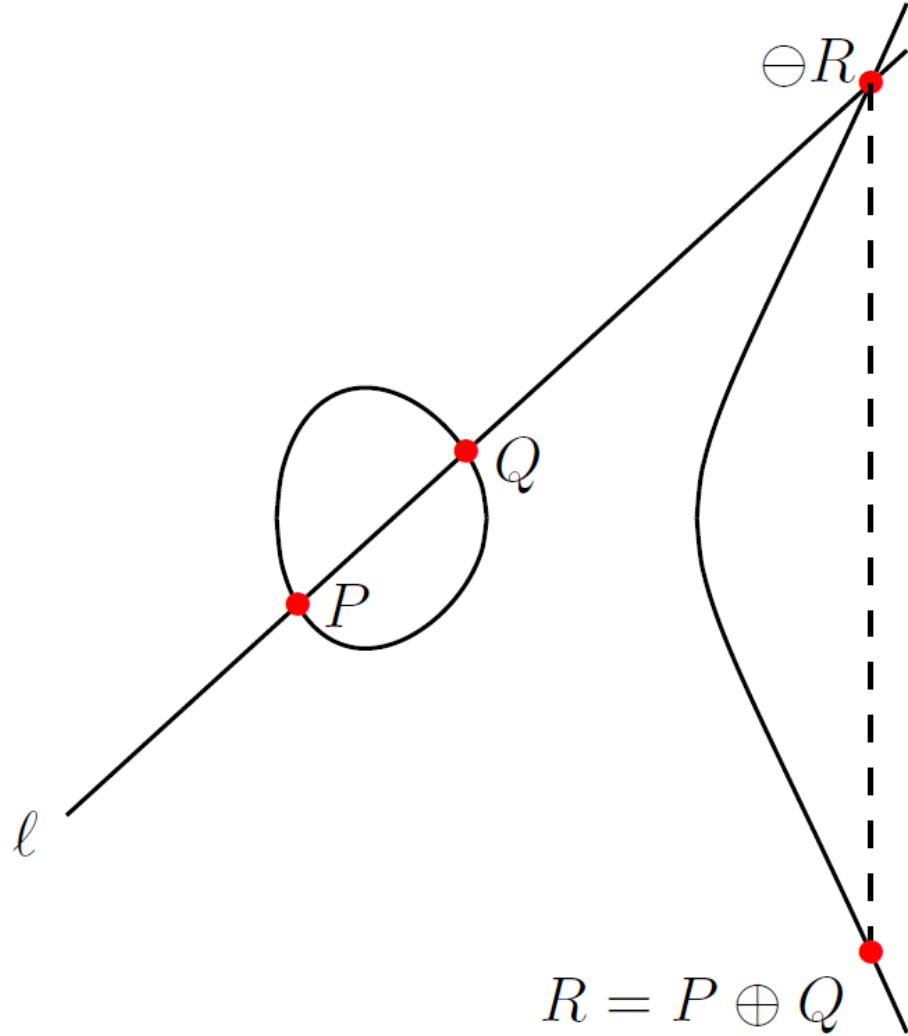
$$x^3 - (\lambda x + \nu)^2 + ax + b = 0$$

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

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

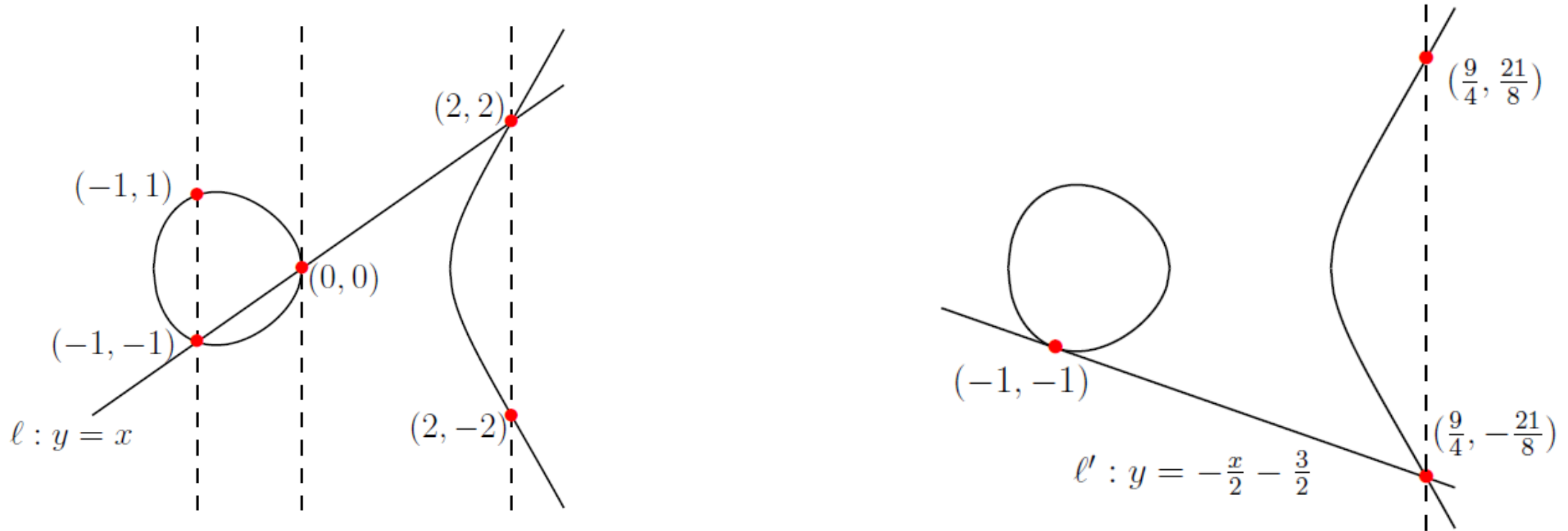
$$y_R = -(\lambda x_R + \nu)$$

The elliptic curve group law \oplus



A toy example

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



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

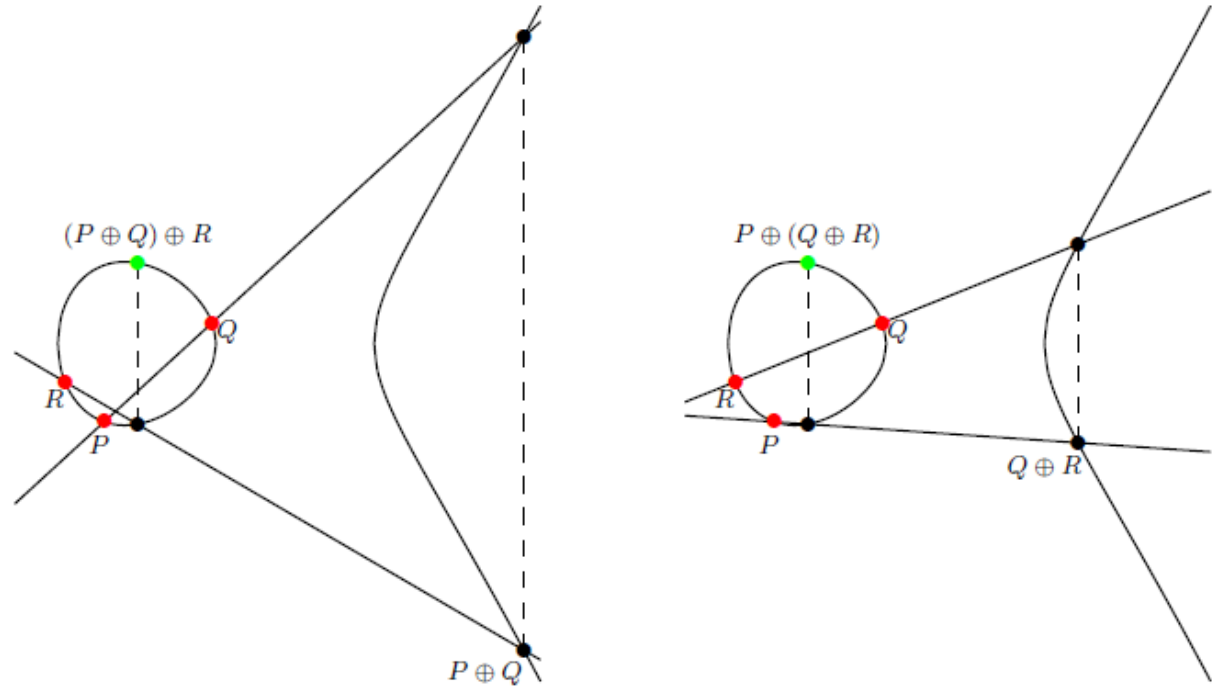
The (abelian) group axioms

- **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:** $\ominus (x, y) = (x, -y)$

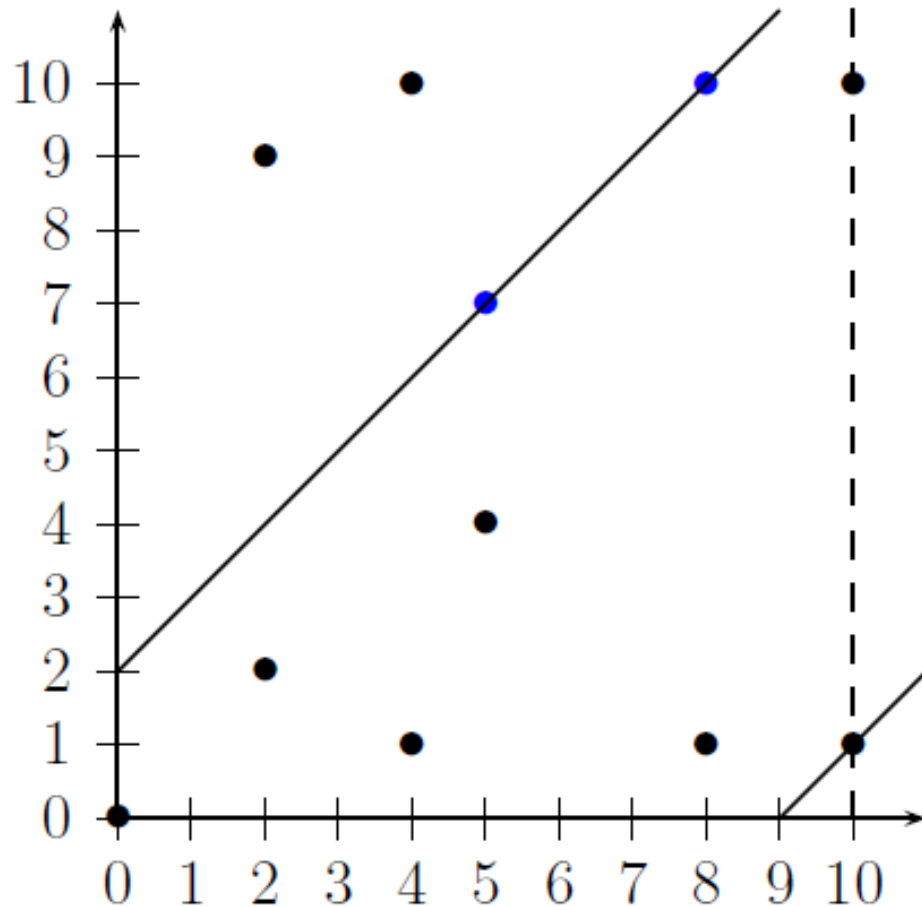
- **Associative:** proof by picture



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

A toy example, cont.

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



$$(7,5) \oplus (8,10) = (10,1)$$

Part 1: Cryptography

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next talk?

Diffie-Hellman key exchange (circa 2016)

$q =$

5809605995369958062859502533304574370686975176362895236661486152287203730997110225737336044533118407251326157754980517443990529594540047121662885672187032401032111639706440498844049850989051627200244765807041812394729680540024104827976584369381522292361208779044769892743225751738076979568811309579125511333093243519553784816306381580161860200247492568448150242515304449577187604136428738580990172551573934146255830366405915000869643732053218566832545291107903722831634138599586406690325959725187447169059540805012310209639011750748760017095360734234945757416272994856013308616958529958304677637019181594088528345061285863898271763457294883546638879554311615446446330199254382340016292057090751175533888161918987295591531536698701292267685465517437915790823154844634780260102891718032495396075041899485513811126977307478969074857043710716150121315922024556759241239013152919710956468406379442914941614357107914462567329693649

$g = 123456789$



g^a
 $(\text{mod } q)$
 $=$

1974966481832271932862620186142505559719097997625337606540081479948757754456670542185781051331382174972068905995549284294506678994768546685955940340934936375624510789382969603134886961788481424913516872530546022029662470461057707715772483216821171742461283211956785376315202786494034647973536919967369935770926871783856022988735589541210564305228996197614537270822178234757462238037900142350513967990494465082246618501681499574014746384567166244019067013944724470150525694177463721850933025357393837919800705723814217290296516393042343612687649717077634843006689239728687091216655686983097865780474015791661156350856988684748772676671207386096152947607114559706340209059103703018182635521898738094546294558035569752596676346614699327742088471255741184755866117812209895514952436160199336532605242210147489825669666012419572610049572551002200293281421876806011231076345540456724876139639963344901857872119208518550803791724

$=$
 g^b
 $(\text{mod } q)$

4116046620695933066832285256534418724107779992205720799935743972371563687620383783327424719396665449687938178193214952698336131699379861648113207956169499574005182063853102924755292845506262471329301240277031401312209687711427883948465928161110782751969552580451787052540164697735099369253619948958941630655511051619296131392197821987575429848264658934577688889155615145050480918561594129775760490735632255728098809700583965017196658531101013084326474277865655251213287725871678420376241901439097879386658420056919119973967264551107584485525537442884643379065403121253975718031032782719790076818413945341143157261205957499938963479817893107541948645774359056731729700335965844452066712238743995765602919548561681262366573815194145929420370183512324404671912281455859090458612780918001663308764073238447199488070126873048860279221761629281961046255219584327714817248626243962413613075956770018017385724999495117779149416882188

$a =$

7147687166405; 957187905360554739658269240518614591652235491261571529709710067917003790492433011601949788108908769613159283138632621095129494458440049748892980385849319181284475723210239871604390620061776483188754575562337708539125052923646318332191217321464134655845254917228378772756695589845219962202945089226665074265269127802446416400\97464722529088780604931795419514638292288904557780459294373052654\10485180264002079415193983851143425084273119820368274789460587100\30497747706924427898968991057212096357725203480402449913844583448

$g^ab =$

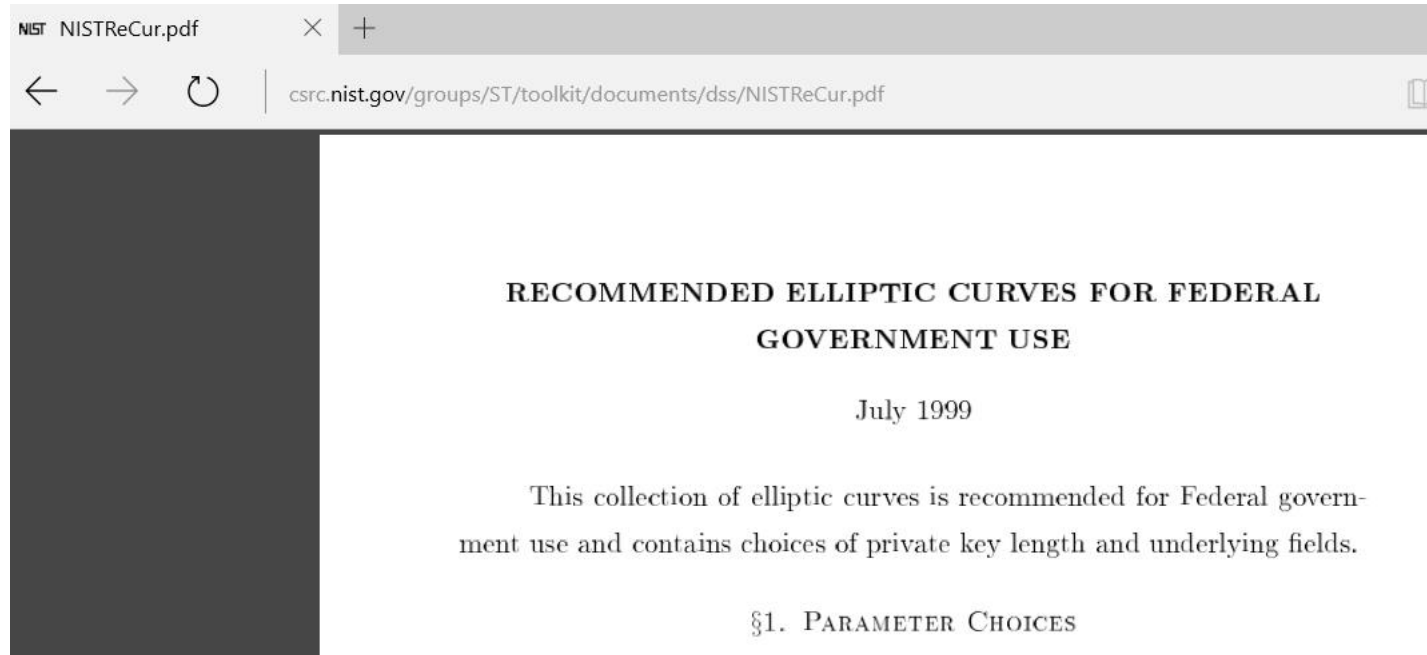
330166919524192149323761733598426244691224199958894654036331526394350099088627302979833339501183059198113987880066739419999231378970715307039317876258453876701124543849520979430233302775032650107245135512092795731832349343596366965069683257694895110289436988215186894965977582185407675178858364641602894716513645524907139614566085360133016497539758756106596557555674744381803579583602267087423481750455634370758409692308267670340611194376574669939893893482895996003389503722513369326735717434288230260146992320711161713922195996910968467141336433827457093761125005143009836512019611866134642676859265636245898172596372485581049036573719816844170539930826718273452528414333373254200883800592320891749460865366649848360413340316504386926391062876271575757583831289710534010374070317315095828076395094487046179839301350287596589383292751993079161318839043121329118930009948197899907586986108953591420279426874779423560221038468



$b =$

655456209464694; 93360682685816031704969423104727624468251177438749706128879957701\93698826859762790479113062308975863428283798589097017957365590672\835713863895712246676094993008985548024464030395443007480025079620363866193152298860635410053224484639158978641210273772558373965\48653931285483865070903191974204864923589439190352993032676961005\08840431979272991603892747747094094858192679116146502863521484987\08623286193422239171712154568612530067276018808591500424849476686\706784051068715397706852664532638332403983747338379697022624261377163163204493828299206039808703403575100467337085017748387148822224875309641791879395483731754620034884930540399950519191679471224\0555855709321935074715577756958163700850920394705281936392411084\43600686183528465724969562186437214972625833222544865996160464558\54622993701658947042526445624157899586972652935647856967092689604\42796501209877036845001246792761563917639959736383038665362727158

NIST Curve P-256



Curve P-256

$p = 11579208921035624876269744694940757353008614\backslash$
3415290314195533631308867097853951

$r = 11579208921035624876269744694940757352999695\backslash$
5224135760342422259061068512044369

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

$c =$ 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



§2. CURVES OVER PRIME FIELDS

For each prime p , a pseudo-random curve

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

ECDH key exchange (1999 – nowish)

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

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

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

$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ 36134250956749795798585127919587881956611106672985015071877198253568414405109)$

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

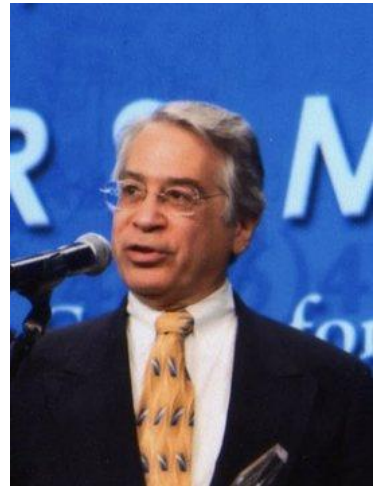
$[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, \\ 77887418190304022994116595034556257760807185615679689372138134363978498341594)$



$a =$

89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

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



$b =$

10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

ECDH key exchange (1999 – nowish)



René Schoof



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

$$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$$

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

$$\#E = 115792089210356248762697446949407573529996955224135760342422259061068512044369$$

$$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ 36134250956749795798585127919587881956611106672985015071877198253568414405109)$$

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

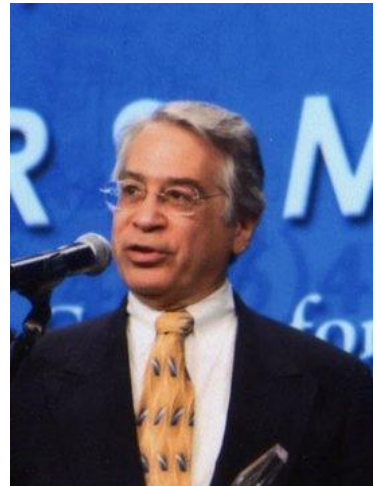
$$[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, \\ 77887418190304022994116595034556257760807185615679689372138134363978498341594)$$



$a =$

89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

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



$b =$

10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

The need for speed

We (practical cryptographers) celebrate the 1%, 2%, 5%, 10% improvements...
... but why???

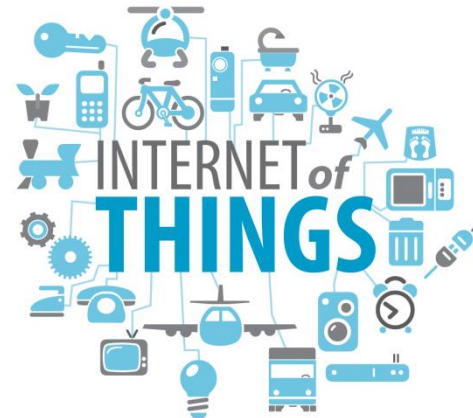
You're browsing MB/GB, what difference does a few extra milliseconds/bytes make?

Here's two reasons:

"the cloud"



"IoT"



Security of the ECDLP

- Given (x_P, y_P) and (x_Q, y_Q) in cyclic elliptic curve group, find the scalar k that relates them ($[k]P = Q$)
- For group of cardinality N , Pollard rho (generic!!!) requires \sqrt{N} steps, e.g. $\#E = 2^{256} \rightarrow 2^{128}$ steps
- Curves provide the only cryptographically useful groups we know that are *as secure as possible*!

ECDH key exchange (1999 – nowish)

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

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

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

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ 36134250956749795798585127919587881956611106672985015071877198253568414405109)$



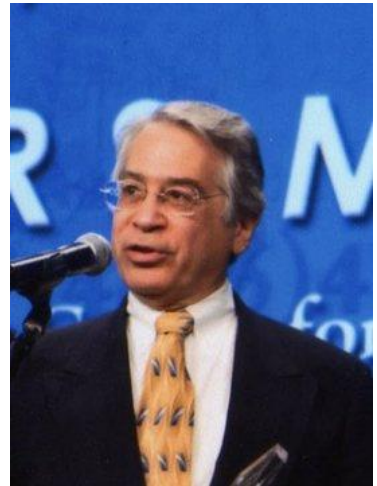
$a =$

89130644591246033577639
77064146285502314502849
28352556031837219223173
24614395

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

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

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



$b =$

10095557463932786418806
93831619070803277191091
90584053916797810821934
05190826

How to compute $k, Q \mapsto [k]Q$?

Scalar multiplications via double-and-add

How to compute $k, Q \mapsto [k]Q$?

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

$$P \leftarrow Q$$

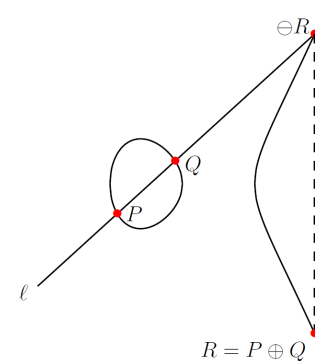
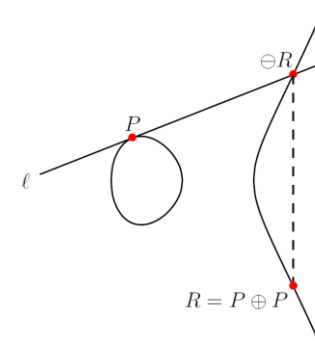
for i from $n - 1$ downto 0 do

$$P \leftarrow [2]P$$

if $k_i = 1$ then

$$P \leftarrow P \oplus Q$$

end for



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

$$\lambda \leftarrow (3x_P^2 + a)/(2y_P); \quad v \leftarrow y_P - \lambda x_P;$$

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

if $k_i = 1$ then

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

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

end for

Projective scalar multiplications

Rather than $(x, y) \in \mathbb{A}^2$, take $(X:Y:Z) \in \mathbb{P}^3$
 $(X:Y:Z) \sim (\lambda X : \lambda Y : \lambda Z)$

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

for i from $n - 1$ downto 0 do

$$(X_P:Y_P:Z_P) \leftarrow [2](X_P:Y_P:Z_P) \quad \mathbf{7M}$$

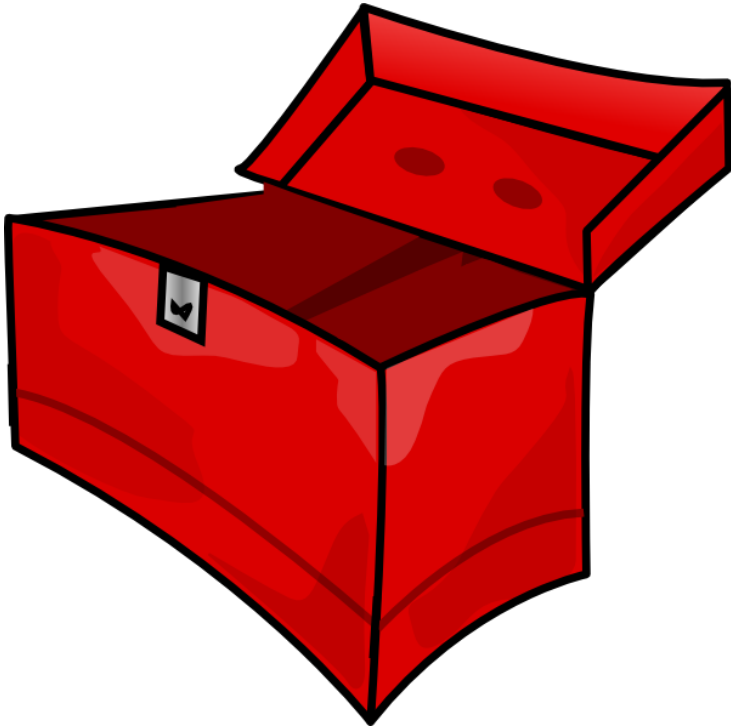
if $k_i = 1$ then

$$(X_P:Y_P:Z_P) \leftarrow (X_P:Y_P:Z_P) + (X_Q:Y_Q:Z_Q) \quad \mathbf{12M}$$

end for

return $(x_P, y_P) \leftarrow (X_P/Z_P, Y_P/Z_P)$

Summary so far: ECC is the best of both worlds



attacker's toolbox

vs.



our toolbox

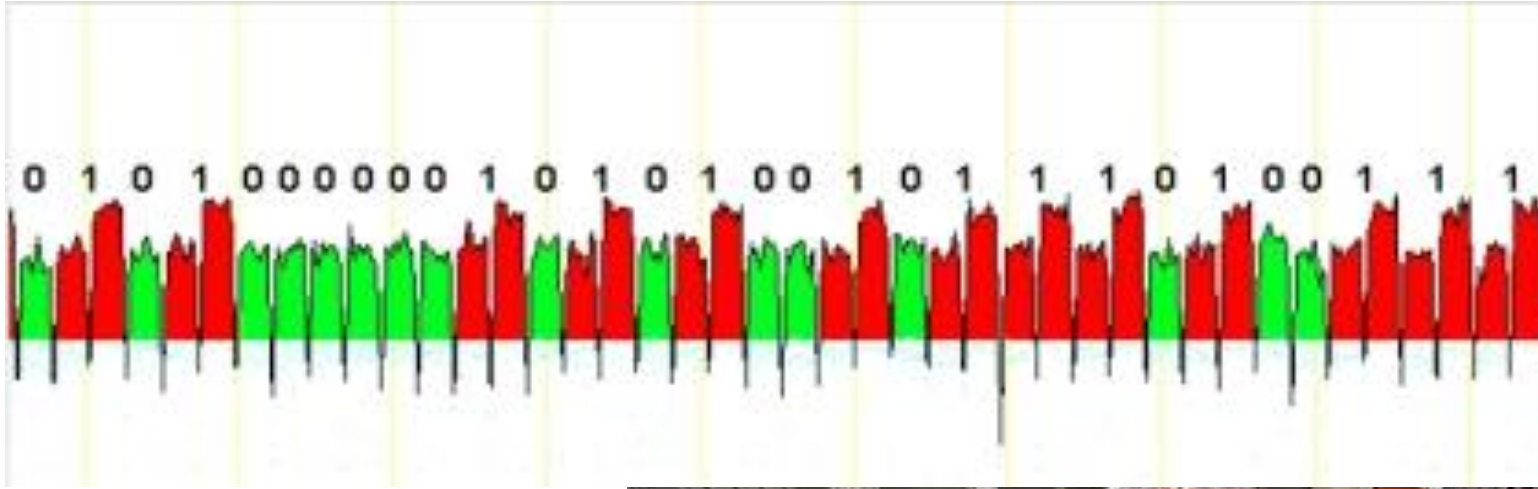
Part 1: Cryptography

Part 2: Elliptic Curves

Part 3: Elliptic Curve Cryptography

Part 4: Next talk?

What's happened since 1999?



June 2013: The Snowden Leaks

Corollary 48.1.2.6:



Conjecture 48.1.2.7:

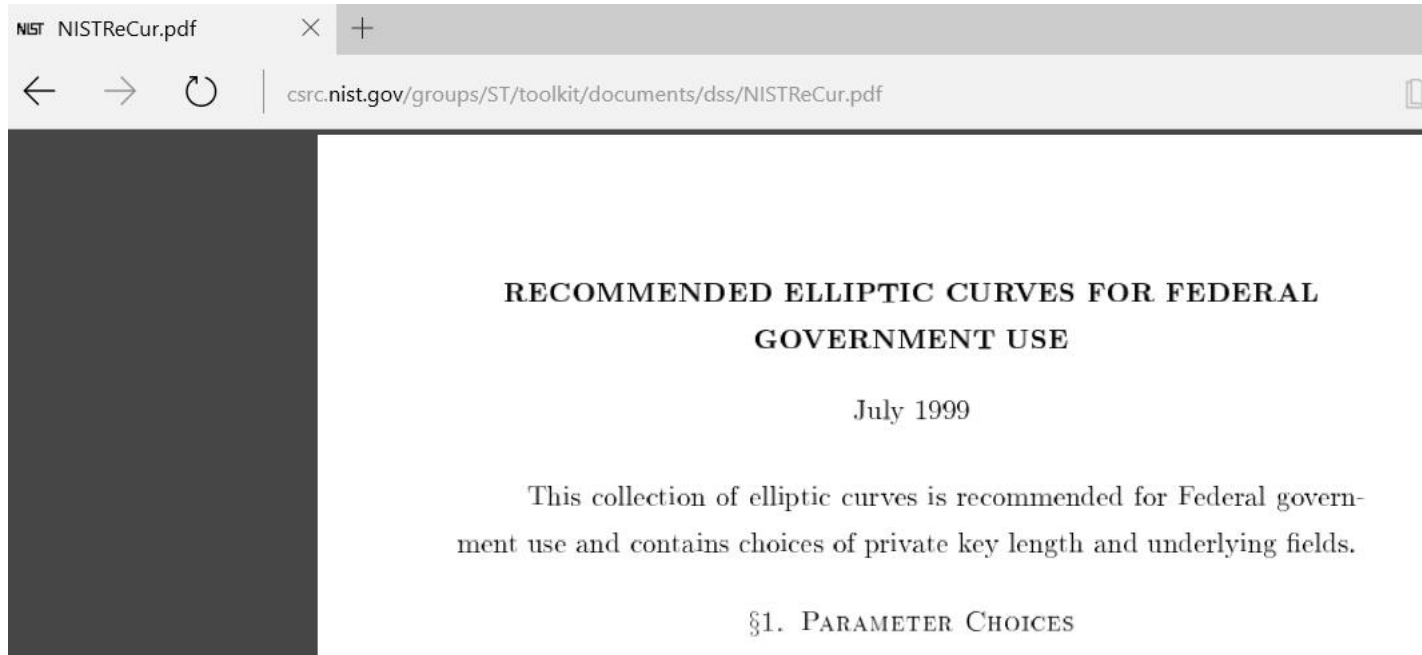
The New York Times

Snowden leaks confirm that the Dual EC DRBG was backdoored by the NSA...

Pretty much everyone.

The NSA could have backdoored the NIST curves.

NSA Curve P-256???



§2. CURVES OVER PRIME FIELDS

For each prime p , a pseudo-random curve

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

Curve P-256

$p =$ 11579208921035624876269744694940757353008614\
3415290314195533631308867097853951

$r =$ 11579208921035624876269744694940757352999695\
5224135760342422259061068512044369

$s =$ 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

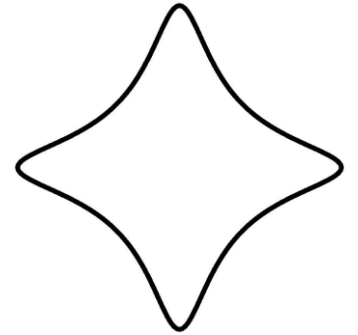


Bruce Schneier

"I no longer trust the constants. I believe the NSA has manipulated them"

Next-generation ECC:

- TLS working group: formal request for new curves
- NIST: reopens "FIPS-186" (ECC Standard)




The Register
Biting the hand that feeds IT

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

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


More like this

Cryptography Nist

Joining the dots of IT delivery
When DevOps meets hybrid cloud
sponsored by IBM
18 November | 11 GMT
REGISTER HERE **LIVE**

Most read

Facebook conjures up a



| Platform | FourQ C-Longa'15 | Curve25519 Bernstein'06 [Cho15] | NIST p-256 NIST'99 [GK15] |
|---------------|---------------------|---------------------------------------|---------------------------------|
| Atom Pineview | 442 | 1,109 | - |
| Intel Sandy | 74 | 157 | 400 |
| Intel Ivy | 71 | 159 | - |
| Intel Haswell | 59 | 162 | 312 |
| AMD Kaveri | 122 | 301 | - |

Speed (in thousands of cycles) of $k, P \mapsto [k]P$ on some 64-bit platforms.

Quantum computers ↔ Cryptopocalypse



- Quantum computers break elliptic curves, finite fields, factoring, everything currently used for PKC



- Aug 2015: NSA announces plans to transition to quantum-resistant algorithms



- Feb 2016: NIST calls for quantum-secure submissions

Post-quantum crypto

- Post-quantum key exchange from ring-LWE
- i.e., securing the web using (\approx) linear algebra...
- Other works in progress...

Cryptographers aim to future-proof protocol

THE AUSTRALIAN | AUGUST 18, 2015 12:00AM



Jennifer Foreshow
Technology reporter
Sydney



Queensland University of Technology's Douglas Stebila and his team are upgrading encryption protocols.

The need to secure today's communications from the powerful quantum computers of the future has propelled new research aimed at upgrading the internet's core encryption protocol.

This work is being led by a team of cryptographers, including Queensland University of Technology's Douglas Stebila, that has tested some new techniques and found

[Log in / Register](#) [Search Q](#)

[Subscribe](#)

[Topics+](#) [The Daily](#) [Magazine](#) [Business Reports](#) [More+](#)

**MIT
Technology
Review**

Computing

**Securing Today's
Data Against
Tomorrow's
Quantum Computers**

Call it an abundance of caution. A Microsoft research project has upgraded the encryption protocol that secures the Web to resist attacks from quantum computers—machines that are expected to have stupendous power but have never been built.

Governments and computing giants like IBM, Microsoft, and Google are working on quantum computers because tapping subtle effects of quantum physics should let them solve in seconds some problems that a conventional machine couldn't solve in billions of years (see "[Microsoft's Quantum Mechanics](#)"). That might allow breakthroughs in areas such as medicine or energy. But such machines would also be able to easily break the encryption used to secure information online.

Next talk?

- **Option 1: FourQ** - the fastest curve on the planet

C-Longa'15: FourQ: four-dimensional decompositions on a Q-curve over the Mersenne prime.

AsiaCrypt 2015. http://link.springer.com/article/10.1007/978-3-662-48797-6_10

- **Option 2: Lattice-based post-quantum cryptography**

Bos-C-Naehrig-Steibla'15: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. IEEE Security & Privacy, 2015. DOI: [10.1109/SP.2015.40](https://doi.org/10.1109/SP.2015.40)

- **Option 3: Fast cryptography in genus 2**

Bos-C-Hisil-Lauter'16: Fast cryptography in genus 2. Journal of Cryptology, 2016.

<http://link.springer.com/article/10.1007/s00145-014-9188-7>

C-Hisil'16: Jacobian coordinates on genus 2 curves. Journal of Cryptology, 2016.

<http://link.springer.com/article/10.1007/s00145-016-9227-7>