Elliptic Curve Cryptography

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

20.03.2009

Data Protection

Many factors influence the security and privacy of data

- Secure storage, physical security.
- Access control.
- Protection against alteration of data
  $\Rightarrow$ digital signatures, message authentication codes.
- Protection of sensitive content against reading
  $\Rightarrow$ encryption.

Cryptology is the science that studies mathematical techniques in order to provide secrecy, authenticity and related properties for digital information.

Different methods for encryption

- Partners share a secret (key)
  $\Rightarrow$ can use symmetric encryption methods
  - classical methods (Caesar, ...) belong to this class
  - one-time pad
  - AES, stream ciphers
- Partners have no initial secret
  $\Rightarrow$ use of public key cryptography
  (topic of this lecture falls in this category;
  other examples: RSA, ElGamal signatures).

Symmetric methods are faster than public key methods for encryption. Most applications use a combination of both (e.g. public key cryptography is used to define a session key). This is called hybrid encryption.

Public key cryptography

Each user U has *two* keys

- a private key s_U, chosen by him which *never* leaves the secure environment,
- a public key p_U, which is made public in a kind of phone book.
- These keys are linked by a (computational) one-way function; the general principles are public.

- Use public key of recipient to encrypt
  $\Rightarrow$ only recipient knows secret key and can decrypt.
- Sender uses his private key to sign message
  $\Rightarrow$ signature must be due to him as only he knows the secret. Everybody can verify signature using public key.

Tasks of the cryptographer

- Find good candidates for computational one-way functions.
- Look for variants having better performance.
- Analysis of attacks.

Proposed candidates

- Multiplying two integers is easy while factoring is hard (RSA).

  primes $p, q \Rightarrow N = p \cdot q \longleftrightarrow$ integer $N \Rightarrow p, q$.
- Computing scalar multiples in some group is easy while it is hard to find the corresponding scalar given two group elements $\Rightarrow$ discrete logarithm problem (DLP).

  $P \in G$, integer $a \Rightarrow Q = [a]P \longleftrightarrow Q, P \in G \Rightarrow a$.

Diffie-Hellman key exchange

Parameters

$P, \ell = |\langle P \rangle|$

Alice		**Bob**
1. secretly generates $a < |\langle P \rangle|$		1. secretly generates $b < |\langle P \rangle|$
2. computes $Q_1 = [a]P$		2. computes $Q_2 = [b]P$
3. transmits Q_1		3. transmits Q_2
4. computes $[a]Q_2$	$= [ab]P =$	4. computes $[b] \cdot Q_1$

Common Key: the group element $k = [(ab)]P \in G$
can be used in symmetric encryption.

Example: key exchange in $\mathbb{Z}$

Public parameter base $P = 2$ and operation $\cdot$ (multiplication).

- First step
  - A chooses a secret number $s_a = 7$
  - B chooses a secret number $s_b = 9$
- second step
  - A computes 2^7 and sends $p_a = 128$
  - B computes 2^9 and sends $p_a = 512$
- third step
  - A computes ${p_B}^7 = 512^7 = 2^{63}$
  - B computes ${p_A}^9 = 128^9 = 2^{63}$

Example: key exchange in $\mathbb{Z}$

Public parameter base $P = 2$ and operation $\cdot$ (multiplication).

- First step
  - A chooses a secret number $s_a = 7$
  - B chooses a secret number $s_b = 9$
- second step
  - A computes 2^7 and sends $p_a = 128$
  - B computes 2^9 and sends $p_a = 512$
- third step
  - A computes ${p_B}^7 = 512^7 = 2^{63}$
  - B computes ${p_A}^9 = 128^9 = 2^{63}$

Problem: Size reveals secret!

What went wrong?

- Actually, the integers $\mathbb{Z}$ do not fit our description since $\langle 2 \rangle = \infty$, so the size of the powers grows with the exponent.
- Key exchange only needs semi-group – but finiteness is important.
- Solution: use modular arithmetic.
  Additionally agree on a prime p such that all computations are done mod p. E.g. use $p = 97$. Then
  $$p_A = 128 - 97 = 31,$$
  $$p_B = 512 - 5 \cdot 97 = 27,$$
  and the joint secret key is
  $$p_B^7 = 27^7 \equiv 79 \equiv 31^9 \bmod 97.$$
- Now each value is bounded by 97, so p_A and p_B do not automatically reveal the secret keys s_A and s_B.

Even more could go wrong

- How about we choose $p = 127$ instead of $p = 97$? Powers of 2 are: $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64, 2^7 = 128 \equiv 1 \bmod 127, 2^8 = 2^7 \cdot 2 \equiv 2 \bmod 127, 2^9 \equiv 2^2 \bmod 127$, etc.
- Powers of 2 modulo 127 take values in a very small set $\{1, 2, 4, 8, 16, 32, 64\}$, so the key shared by Alice and Bob is one of these 7 values – instead of the 126 different values that one could have hoped for. An attacker can simply try all of them.
- Of course 127 is also much too small to avoid attacks; at least 1024 bits are needed for p and good security requires at least 2048 bits for p. Beyond that the number of different powers obtainable from a chosen base must be sufficiently large – at least 2^{160} for low security and 2^{224} to match the 2048 bits.

Proposed groups

- Integers modulo prime $\mathbb{F}_p^*$.
- Arbitrary finite fields $\mathbb{F}_q^*$.
- Points on elliptic curve over finite field.
- Jacobian of hyperelliptic curve over finite field.

Difference in security:

- first two examples have subexponential algorithms

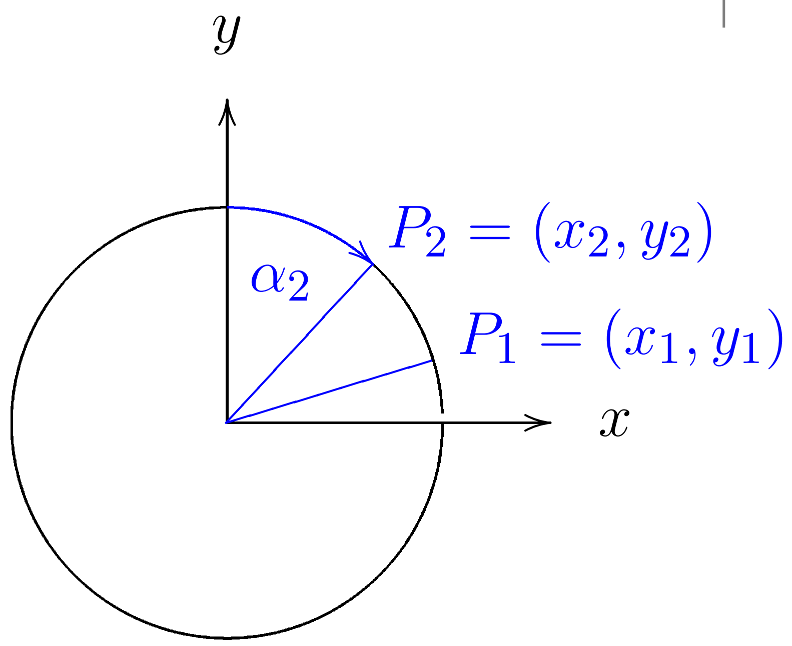
$$O(\exp(c(\log q)^{1/3}(\log\log q)^{2/3})).$$

- For elliptic and small genus hyperelliptic curves the best algorithms are exponential

$$O(\exp(1/2\log \ell)) = O(\ell^{1/2}).$$

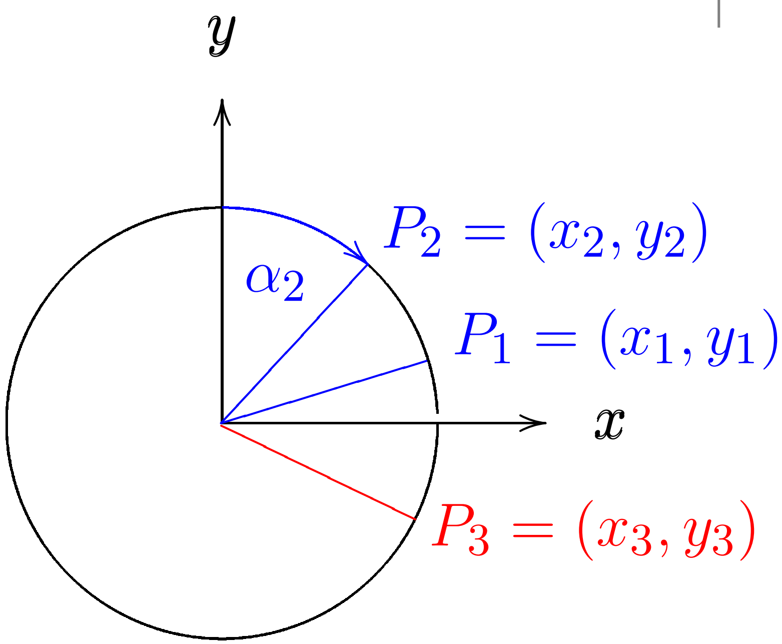
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



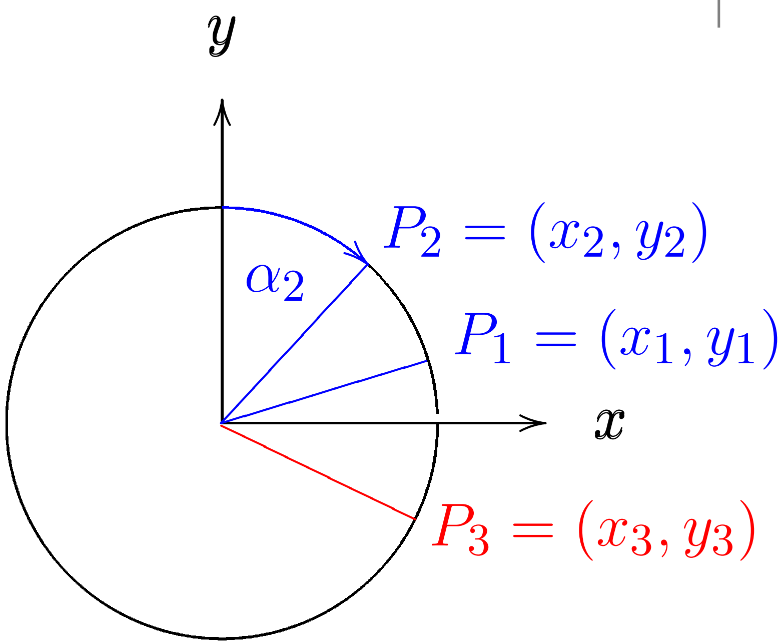
Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$



Do you know how to add on a circle?

Let k be a field with $2 \neq 0$.
Circle: $\{(x, y) \in k \times k | x^2 + y^2 = 1\}$
$x_i = \sin(\alpha_i),\ y_i = \cos(\alpha_i)$



$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \end{aligned}$$

$$\begin{aligned} y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \end{aligned}$$

Addition of angles defines commutative group law
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

DH-key exchange on circle I

- Can do the key exchange on circle.
- $P = (0, 1)$ is on curve at $\alpha = 0$. Then $[2]P$ is at angle $2 \cdot 0$, so $[2]P = P$. Same with formulas.
- If we add $P = (0, 1)$ and $Q = (x_2, y_2)$ we get

  $$x_3 = 0 \cdot y_2 + 1 \cdot x_2 = x_2 \text{ and } y_3 = 1 \cdot y_2 - 0 \cdot x_2 = y_2,$$

  so $(0, 1) + Q = Q$; also $Q + (0, 1) = Q$. An element which does not alter the second input upon addition is called neutral element.
- Other points: e.g. $R = (0, -1)$; this is at angle $180°$. Then $[2]R =?$

DH-key exchange on circle I

- Can do the key exchange on circle.
- $P = (0, 1)$ is on curve at $\alpha = 0$. Then $[2]P$ is at angle $2 \cdot 0$, so $[2]P = P$. Same with formulas.
- If we add $P = (0, 1)$ and $Q = (x_2, y_2)$ we get

  $$x_3 = 0 \cdot y_2 + 1 \cdot x_2 = x_2 \text{ and } y_3 = 1 \cdot y_2 - 0 \cdot x_2 = y_2,$$

  so $(0, 1) + Q = Q$; also $Q + (0, 1) = Q$. An element which does not alter the second input upon addition is called neutral element.
- Other points: e.g. $R = (0, -1)$; this is at angle $180°$. $x_3 = 0 \cdot (-1) + (-1) \cdot 0 = 0$ and $y_3 = (-1) \cdot (-1) - 0 \cdot 0 = 1$. Thus $[2]R = (0, 1)$. This means that multiples of R have only two different values – R and $(0, 1)$, the neutral element. The smallest number n needed to have $[n]R = (0, 1)$ is called the order of R.

DH-key exchange on circle II

- What is the order of $(1,0)$?

DH-key exchange on circle II

- What is the order of $(1, 0)$? $[2](1, 0)$ has $x_3 = 1 \cdot 0 + 0 \cdot 1 = 0$ and $y_3 = 0 \cdot 0 - 1 \cdot 1 = -1$ and we know that $[2](0, -1) = (0, 1)$. So $[2]([2](1, 0)) = [4](1, 0)$ and the order of $(1, 0)$ is 4.

DH-key exchange on circle II

- What is the order of $(1,0)$? $[2](1,0)$ has $x_3 = 1\cdot 0 + 0\cdot 1 = 0$ and $y_3 = 0\cdot 0 - 1\cdot 1 = -1$ and we know that $[2](0,-1) = (0,1)$. So $[2]([2](1,0)) = [4](1,0)$ and the order of $(1,0)$ is 4.
- Negative of (x,y) is $(-x,y)$, this means $(x,y)+(-x,y) = (0,1)$. Test: $x_3 = x\cdot y + y\cdot(-x) = 0$, $y_3 = y\cdot y - x\cdot(-x) = y^2 + x^2 = 1$ (circle equation).
- These observations are clear from the angles on the circle, e.g. the point $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is on the circle at 45° and so the point has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$?

DH-key exchange on circle II

- What is the order of $(1,0)$? $[2](1,0)$ has $x_3 = 1 \cdot 0 + 0 \cdot 1 = 0$ and $y_3 = 0 \cdot 0 - 1 \cdot 1 = -1$ and we know that $[2](0,-1) = (0,1)$. So $[2]([2](1,0)) = [4](1,0)$ and the order of $(1,0)$ is 4.
- Negative of (x,y) is $(-x,y)$, this means $(x,y)+(-x,y) = (0,1)$. Test: $x_3 = x \cdot y + y \cdot (-x) = 0$, $y_3 = y \cdot y - x \cdot (-x) = y^2 + x^2 = 1$ (circle equation).
- These observations are clear from the angles on the circle, e.g. the point $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ is on the circle at $45°$ and so the point has order 8.
- How about $S = (\frac{3}{5}, \frac{4}{5})$? Compute $[2]S$:

$$x_3 = \frac{3}{5}\frac{4}{5} + \frac{4}{5}\frac{3}{5} = \frac{24}{25},\ y_3 = \frac{4}{5}\frac{4}{5} - \frac{3}{5}\frac{3}{5} = \frac{7}{25}$$

$[3]S = [2]P + P$: $x_3 = \frac{24}{25}\frac{4}{5} + \frac{7}{25}\frac{3}{5} = \frac{103}{125},\ y_3 = \frac{7}{25}\frac{4}{5} - \frac{24}{25}\frac{3}{5} = \frac{-54}{125}$.

DH-key exchange on circle III

- No obvious order. Actually there are infinitely many points with x and y coordinates in the reals $\mathbb{R}$.
- Use lessons learned before and choose integers modulo prime p' as space for the coordinates.
- The system has the same security as the one before for primes of half the bit size. However, at the same time the group operations are more involved. How many multiplications do you need to compute

$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2?$$

DH-key exchange on circle III

- No obvious order. Actually there are infinitely many points with x and y coordinates in the reals $\mathbb{R}$.
- Use lessons learned before and choose integers modulo prime p' as space for the coordinates.
- The system has the same security as the one before for primes of half the bit size. However, at the same time the group operations are more involved. How many multiplications do you need to compute

  $$x_3 = x_1y_2 + y_1x_2 \text{ and } y_3 = y_1y_2 - x_1x_2?$$

  3 multiplications! Compute $A = x_1 \cdot x_2,\ B = y_1 \cdot y_2$ and $C = (x_1 + y_1) \cdot (x_2 + y_2) = x_1x_2 + y_1y_2 + x_1y_2 + y_1x_2$.

DH-key exchange on circle III

- No obvious order. Actually there are infinitely many points with x and y coordinates in the reals $\mathbb{R}$.
- Use lessons learned before and choose integers modulo prime p' as space for the coordinates.
- The system has the same security as the one before for primes of half the bit size. However, at the same time the group operations are more involved. How many multiplications do you need to compute

  $$x_3 = x_1y_2 + y_1x_2 \text{ and } y_3 = y_1y_2 - x_1x_2?$$

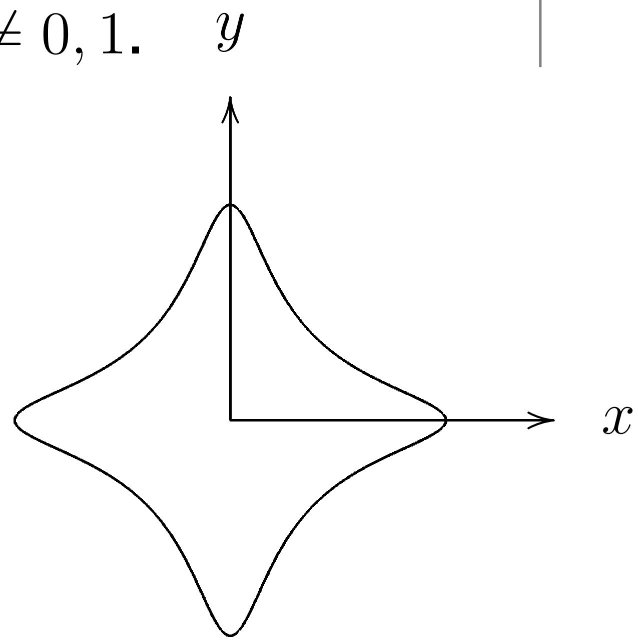
  3 multiplications! Compute $A = x_1 \cdot x_2,\ B = y_1 \cdot y_2$ and $C = (x_1 + y_1) \cdot (x_2 + y_2) = x_1x_2 + y_1y_2 + x_1y_2 + y_1x_2$.
  Then $x_3 = C - A - B,\ y_3 = B - A$.
- Depending on implementation, 3M modulo p' might be favorable to 1M modulo p

Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$

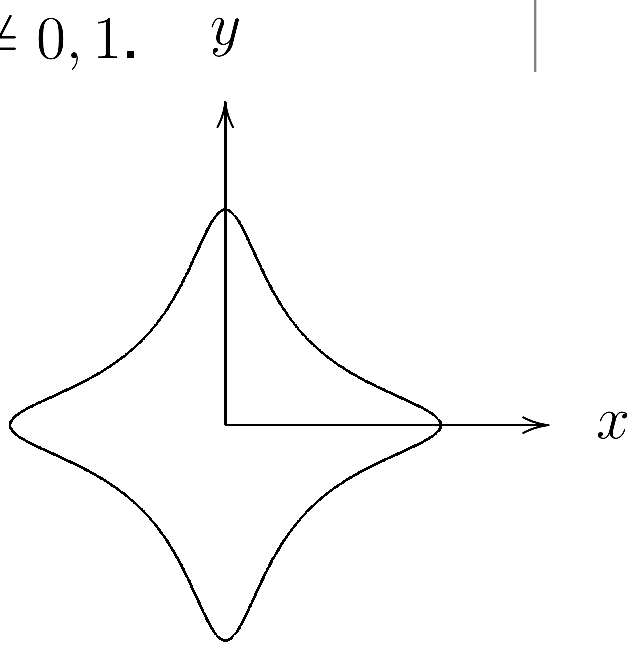
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

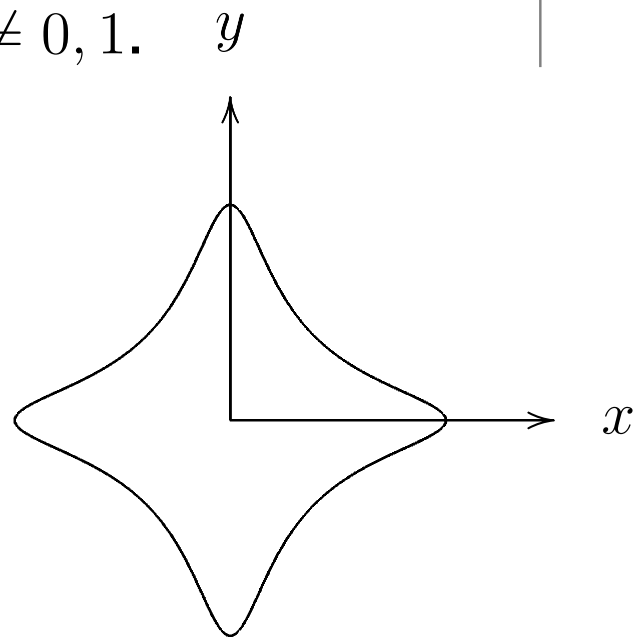
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

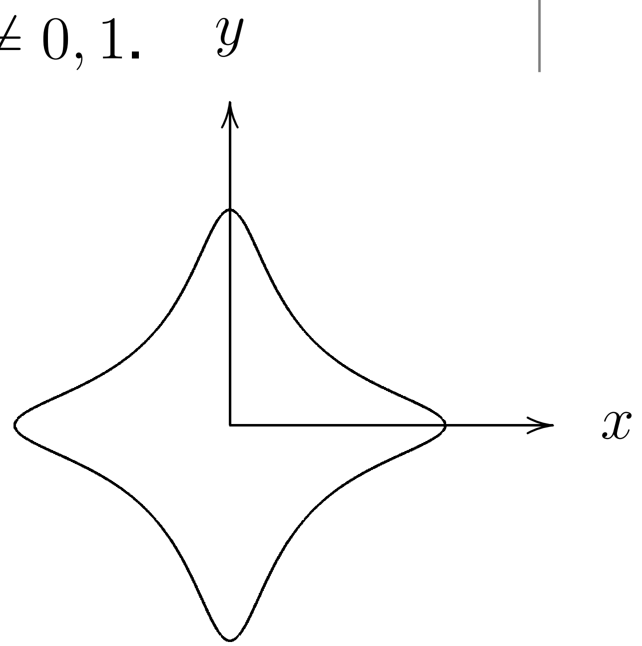
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

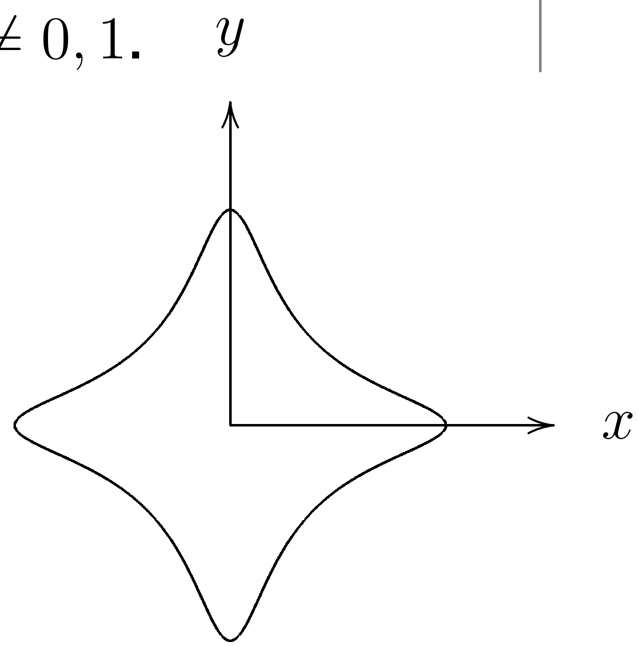
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).

Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

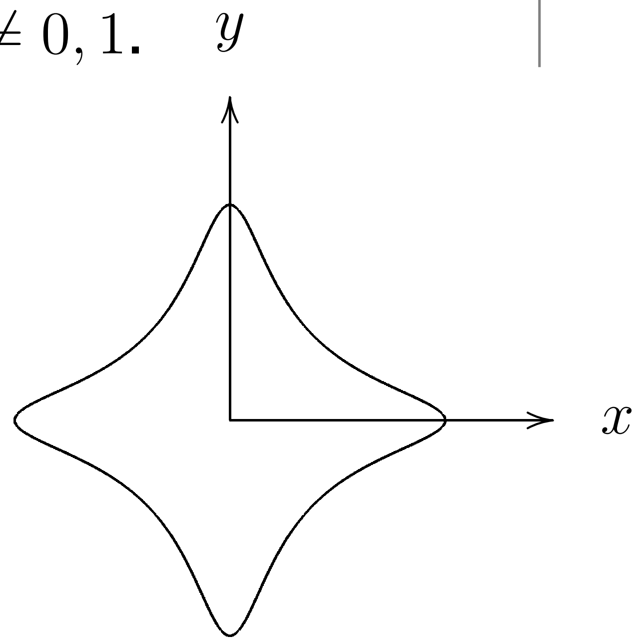
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).
- $-(x_1, y_1) =$

Now add on an elliptic curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve (nice form of elliptic curve):

$$\{(x, y) \in k \times k | x^2 + y^2 = 1 + dx^2y^2\}$$



Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)

Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is $(0, 1)$ (like on circle).
- $-(x_1, y_1) = (-x_1, y_1)$ (like on circle).

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $$P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2},\frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$$
- $$[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1},\frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0,1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $$P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$$
- $$[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

Nice features of the addition law

- Neutral element of addition law is affine point, this avoids special routines (for $(0, 1)$ one of the inputs or the result).
- Addition law is symmetric in both inputs.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

Explicit formulas: addition

- $(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$.
- Avoid inversions: Use $(X_1 : Y_1 : Z_1)$ with $Z_1 \neq 0$ to represent $(x_1, y_1) = (X_1/Z_1, Y_1/Z_1)$, i. e., $(X_1 : Y_1 : Z_1) = (\lambda X_1 : \lambda Y_1 : \lambda Z_1)$ for $\lambda \neq 0$.
- Addition formulas in projective coordinates:

$$\begin{aligned}
A &= Z_1 \cdot Z_2;\ B = A^2;\ C = X_1 \cdot X_2;\ D = Y_1 \cdot Y_2; \\
E &= d \cdot C \cdot D;\ F = B - E;\ G = B + E; \\
X_3 &= A \cdot F \cdot ((X_1 + Y_1) \cdot (X_2 + Y_2) - C - D); \\
Y_3 &= A \cdot G \cdot (D - C); \\
Z_3 &= F \cdot G.
\end{aligned}$$

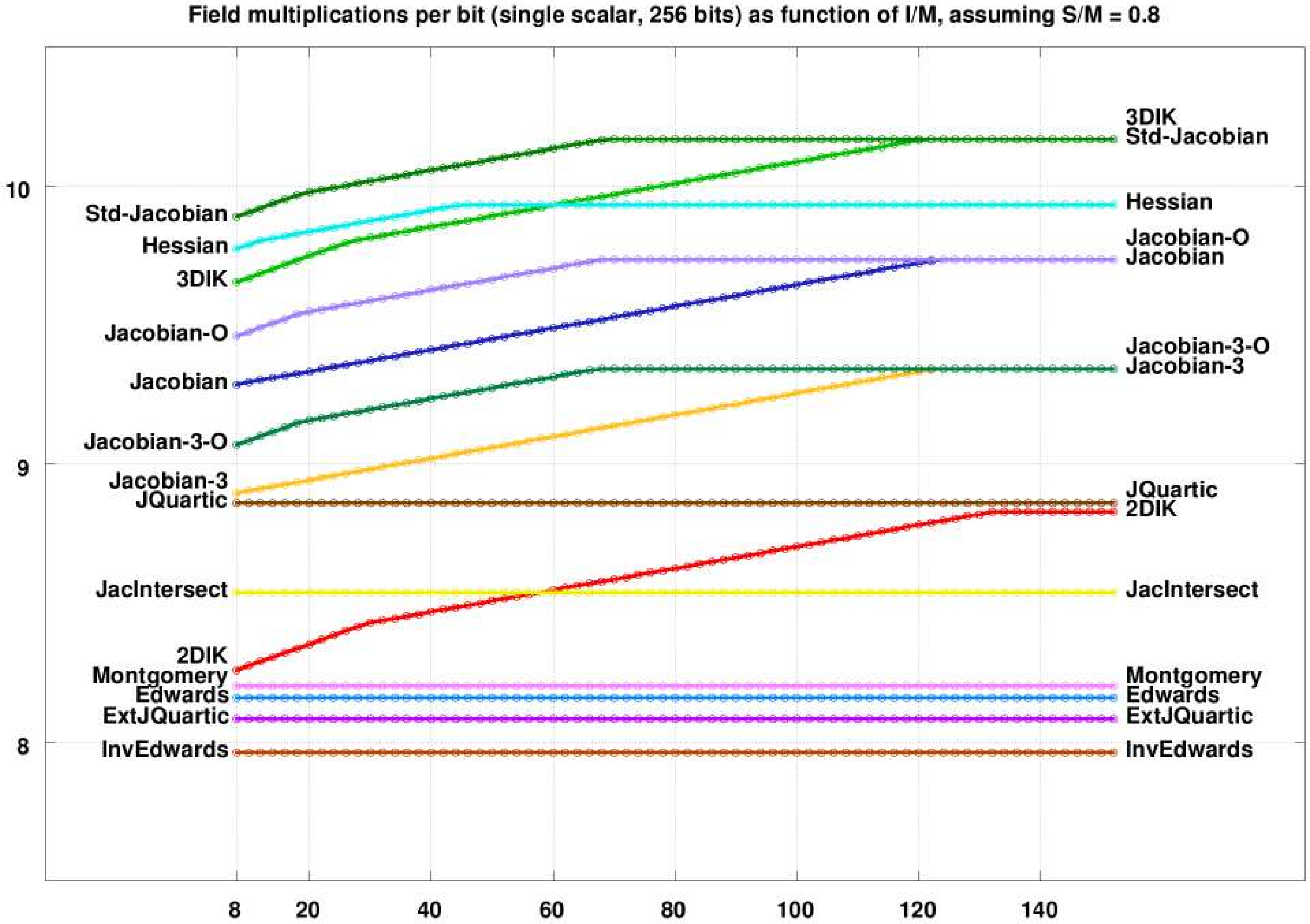
- Needs 10M + 1S + 1D + 7A. This sounds like a lot – but primes have size 160–224 bits. Paranoid: 256 bits.

Complete addition law

- For d not a square in k, the Edwards addition law is complete, there are no exceptional cases.
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on curve.
  - Addition works to add P and P.
  - Addition works to add P and $-P$.
  - Addition just works to add P and any Q.
- Only complete addition law in the literature.
- Very fast point addition 10M + 1S + 1D.
- Dedicated doubling formulas need only 3M + 4S.
- Fastest scalar multiplication in the literature, in particular in 'Inverted Edwards' representation.

Speed comparison & influence of inversions

Different ways to write elliptic curve have different speeds.



Consequences

- Faster arithmetic than on other representations of elliptic curves; also much faster than RSA or computations in $\mathbb{F}_p^*$ at same security level.
- Speed records for Diffie-Hellman key exchange.
- Faster signature computation (additions in this form are easy).
- Can afford larger key length for same speed (or get faster for same level of security).
- Applications using scalar multiplication on elliptic curves get faster . . .

Consequences

- Faster arithmetic than on other representations of elliptic curves; also much faster than RSA or computations in $\mathbb{F}_p^*$ at same security level.
- Speed records for Diffie-Hellman key exchange.
- Faster signature computation (additions in this form are easy).
- Can afford larger key length for same speed (or get faster for same level of security).
- Applications using scalar multiplication on elliptic curves get faster …
- …which also means that attacks using EC arithmetic get faster.
- We have paper at Eurocrypt’09 using Edwards curves for factorization (attacking RSA) on GPUs.

Stay tuned – you'll hear from elliptic curves again

Thanks for your attention!

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve. order 4.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0,0)$. Then Weierstrass form:

$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$

- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy 2)>;

$$x^2 + y^2 = 1 + dx^2y^2.$$

- Inverse map $u = u_4(1 + y)/(1 - y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.