The power of mathematics to protect data and to break data protection

Tanja Lange

Coding Theory and Cryptology

EIPSI

Department of Mathematics and Computer Science

tanja@hyperelliptic.org

17.01.2008

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.

Encryption

Important Distinction

- Partners share a secret (key)
  $\Rightarrow$ use of *symmetric encryption* methods
  - classical methods (Caesar, . . .) belong to this class
  - One-time pad
  - AES
- Partners have no initial secret
  $\Rightarrow$ use of public key cryptography
  - RSA
  - Diffie-Hellman key-exchange
  - ElGamal signatures

Most applications are hybrid, i.e., they use a combination of both (e.g. use public key cryptography to get session key).

Public Key cryptography

Each user has two keys

- a private key chosen by him which *never* leaves the secure environment,
- a public key 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.
- Sender uses 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; every recipient can verify the signature using the sender's public key.

What do mathematicians do here?

- 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).

$$\text{primes } p, q \Rightarrow N = p \cdot q \longleftrightarrow \text{ integer} N \Rightarrow p, q.$$

- In some groups computing scalar multiples is easy while finding the corresponding scalar given two group elements is hard $\Rightarrow$ discrete logarithm problem (DLP).

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

RSA

RSA Cryptosystem I

Secret computation – key generation:

- pick two primes p, q,
- compute $N = p \cdot q$,
- compute $\varphi(N) = (p-1)(q-1)$, where φ is the Euler-φ function,
- pick integer e co-prime to $\varphi(N)$,
- compute d with $de \equiv 1 \bmod \varphi(N)$.

Note that for any m with $\gcd(m, N) = 1$ the order of m modulo N is $\varphi(N)$.
So we have

$$(m^e)^d \equiv m^{ed} \equiv m^{k\varphi(N)+1} \equiv m \bmod N,$$

for some integer k.

RSA Cryptosystem II

- secret key d,
- public key (e, N).
- All intermediate values of the key generation should be deleted.
- Encryption of message m (school-book version!):
  - compute $c \equiv m^e \bmod N$,
  - send ciphertext c.
- Decryption of ciphertext c:
  - compute $c^d \equiv (m^e)^d \bmod N$,
  - obtain cleartext m.

Signature on message m is $m^d \bmod N$. Signing requires knowledge of secret key d.

Parameters & common pitfalls

- Factorization hardest if p and q have same size.
- Current choice: N has 1024 bits and p and q have 512 bits.
- 1024 bits still feel secure, agencies recommend it for documents needing no more than 5 years of security
- Better security 2048 bits and not too painful performance (if one really wants to stick to RSA . . .).
- Problem if one takes 'same size' too literally:

$$
\begin{aligned}
N = {} & 100000000000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000000000\\
& 000000000000000000000000000000000000000000000000000000000000029\\
& 999999999999999999999999999999999999999999999999999999999999999\\
& 999999999999999999999999999999999999999999999999999999999999999\\
& 9999999999999999999999999999999999999999999999999999999997921.
\end{aligned}
$$

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.
- Brute-force search $\gcd(N, 10^{170} - i)$ finds factor $q = 10^{170} - 33$ and then $p = N/q = 10^{170} + 63$.

Pitfalls ctd.

- Yes, this looks like very close to a power of 10, actually close to 10^{340}. Squareroot $\sqrt{N}$ is almost an integer, almost 10^{170}.
- Brute-force search $\gcd(N, 10^{170} - i)$ finds factor $q = 10^{170} - 33$ and then $p = N/q = 10^{170} + 63$.
- This attack is well known and mentioned e.g. in the Handbook of Applied Cryptography. Yet it is found in practice by amateurs, usually with powers of 2 rather than 10.
- Famous example: letter bomber Franz Fuchs in Austria (6 attack series between 1993 and capture in 1997) send RSA-encrypted letter to Austrian magazine 'Profil'. Modulus N had 1024 bits, i.e. full size, but both primes were extremely close to 2^{512}. Found by Hans Dobbertin.

Attacks against generic RSA

Best known attacks against generic RSA try to find a, b with

$$a^2 \equiv b^2 \bmod N, \text{ i.e., } N|(a^2 - b^2). \quad (1)$$

If $N \nmid (a \pm b)$ then

$$1 < \gcd(N, a-b) < N$$

finds nontrivial factor.
The quadratic sieve finds such a relation by computing for many integers a_i

$$(a_i^2 \bmod N) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} a_i', \quad (2)$$

where p_j in factor base F and $\gcd(a_i', p_j) = 1$ for all $p_j \in F$.
Collect relations of form (2) with $a_i' = 1$; construct relation (1) using linear algebra. Number field sieve is similar.

Encryption of long messages

–

need joint secret to use faster symmetric crypto

Diffie-Hellman Key exchange

Alice

1. secretly generates
   $a < |\langle P\rangle|$
2. computes $Q_1 = [a]P$
3. transmits Q_1

Bob

1. secretly generates
   $b < |\langle P\rangle|$
2. computes $Q_2 = [b]P$
3. transmits Q_2

4. computes (Alice)
   $[a]Q_2$

4. computes (Bob)
   $[b] \cdot Q_1$

$$[a]Q_2 = [ab]P = [b] \cdot Q_1$$

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

Proposed groups

- $\mathbb{F}_p^*$, multiplicative group of prime field.
- $\mathbb{F}_q^*$ (same for arbitrary finite field).
- $E(\mathbb{F}_q)$, group of $\mathbb{F}_q$-rational points on elliptic curve E.
- $\mathrm{Pic}_C^0(\mathbb{F}_q)$, divisor class group of curve C over $\mathbb{F}_q$.

Difference in security:

- First two examples have algorithms subexponential in q

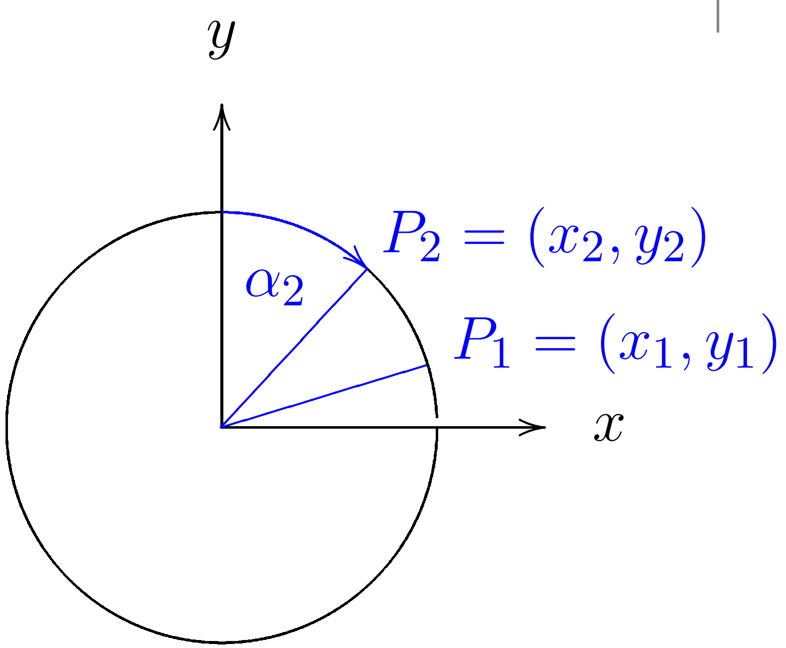
$$O(\exp(c(\log q)^{1/3}(\log\log q)^{2/3})),$$

- for elliptic and small genus hyperelliptic curves the best algorithms are exponential in group size l

$$\Theta(\exp((1/2)\log l)) = \Theta(l^{1/2}).$$

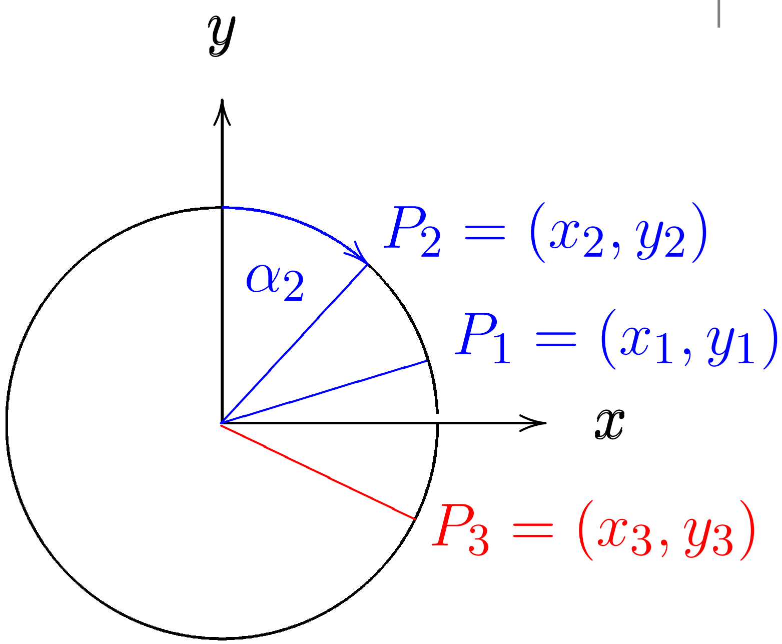
Do you know how to add on a circle?

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



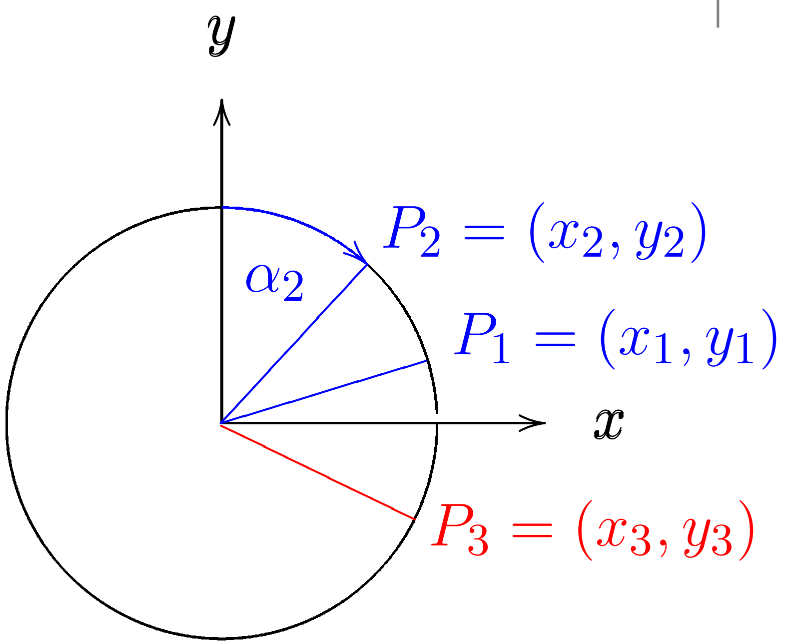
Do you know how to add on a circle?

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

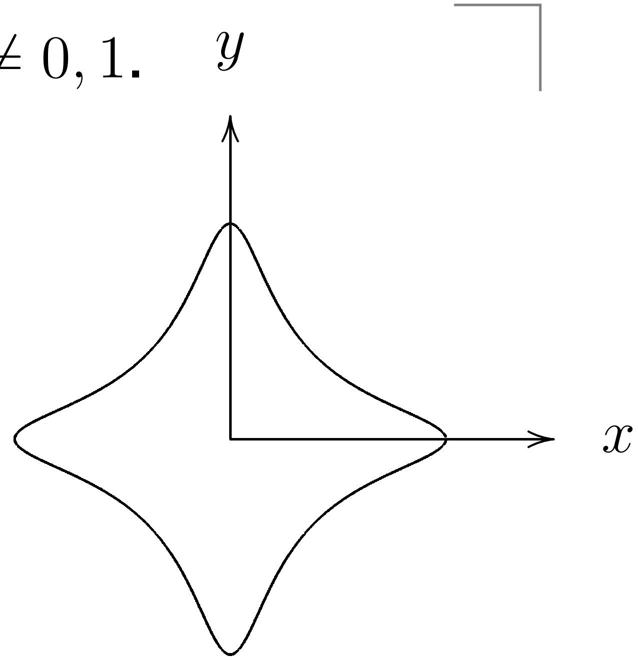
$$x_3 = x_1 y_2 + y_1 x_2 \text{ and } y_3 = y_1 y_2 - x_1 x_2.$$

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards curve:

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

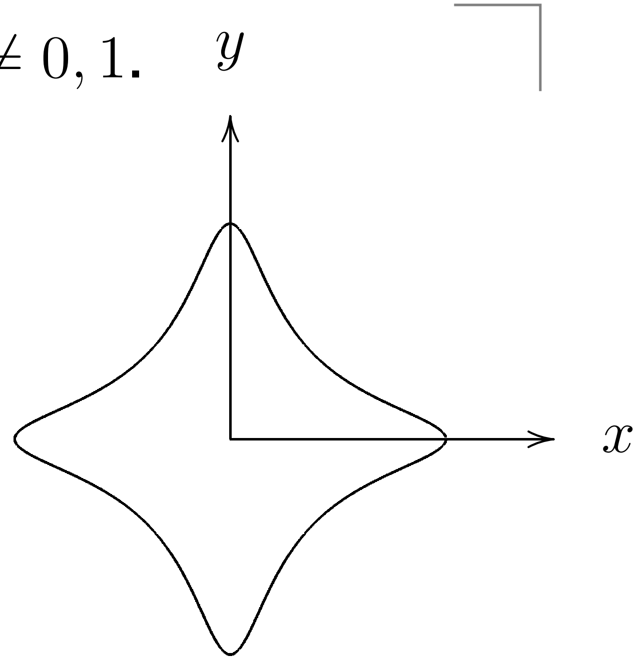
Harold M. Edwards,
(Bulletin of the AMS, **44**, 393–422, 2007)



Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards 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)

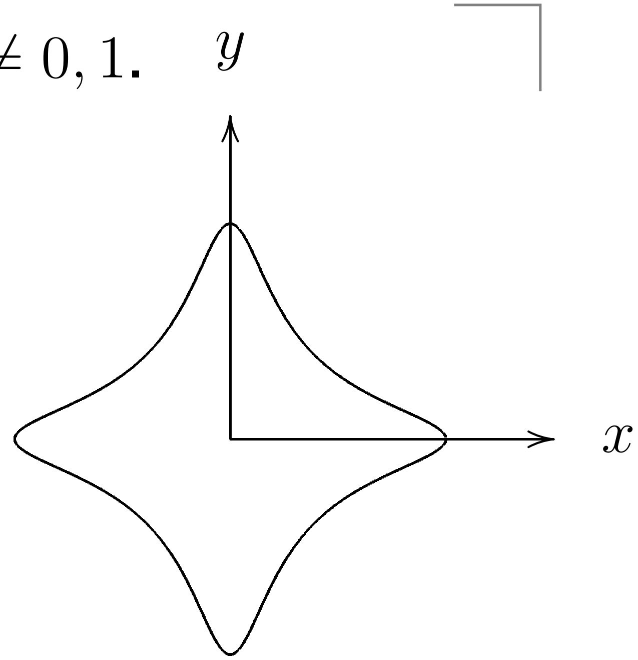
Associative operation on points
$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
defined by Edwards addition law

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

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards 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

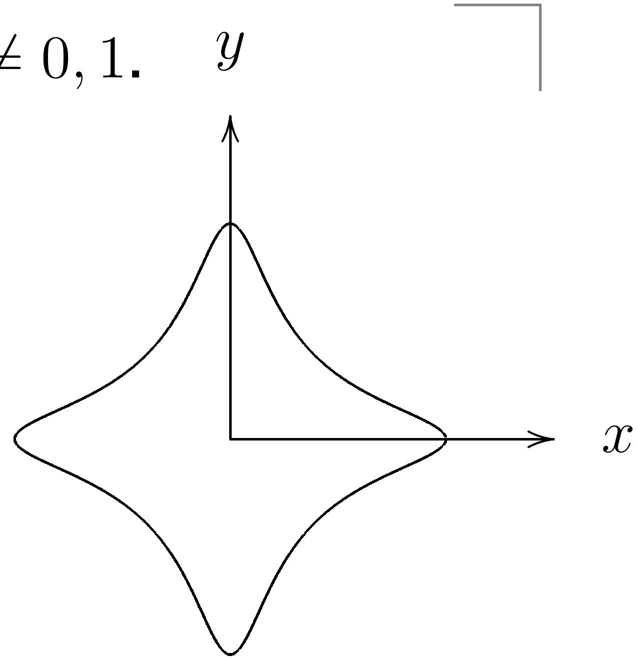
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

- Neutral element is

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards 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

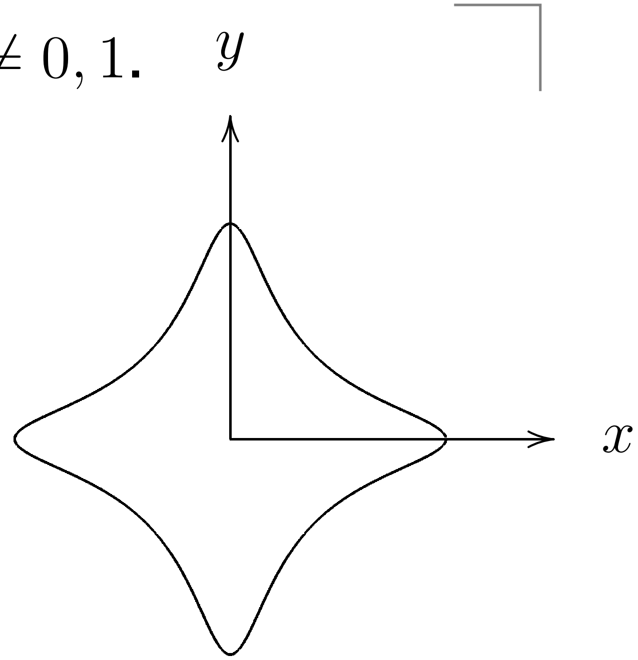
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

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

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards 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

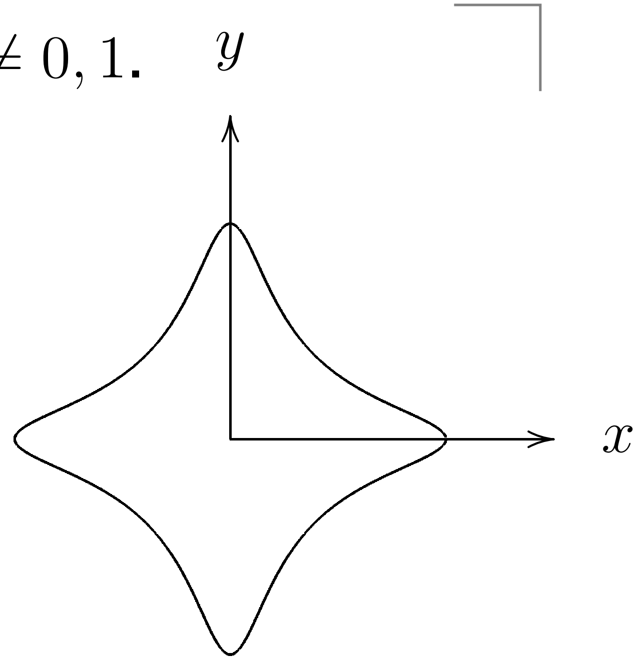
$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \text{ and } y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}.$$

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

Now add on an Edwards curve

Let k be a field with $2 \neq 0$. Let $d \in k$ with $d \neq 0, 1$.
Edwards 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).

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- 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
$$x^2 + y^2 = 1 + dx^2y^2.$$
- Inverse map $u = u_4(1 + y)/(1 - y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.

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.
- $P + Q = \left(\dfrac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \dfrac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$

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.
- $P + Q = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right).$
- $[2]P = \left(\frac{x_1 y_1 + y_1 x_1}{1 + d x_1 x_1 y_1 y_1}, \frac{y_1 y_1 - x_1 x_1}{1 - d x_1 x_1 y_1 y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.

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.
- $P + Q = \left(\dfrac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \dfrac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$
- $[2]P = \left(\dfrac{x_1y_1 + y_1x_1}{1 + dx_1x_1y_1y_1}, \dfrac{y_1y_1 - x_1x_1}{1 - dx_1x_1y_1y_1} \right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!

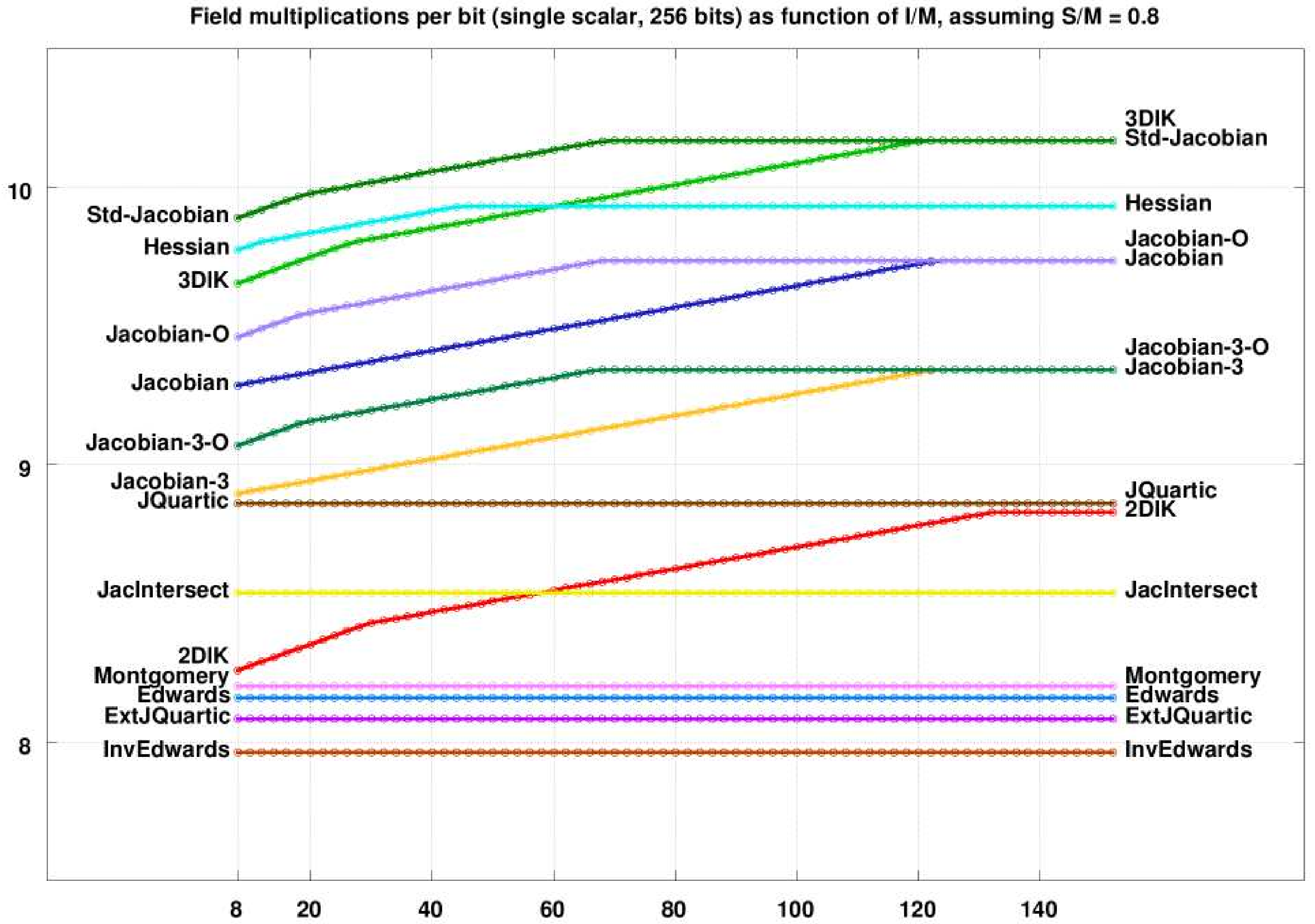
Nice features of the addition law

- 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.
- $P+Q=\left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
- $[2]P=\left(\frac{x_1y_1+y_1x_1}{1+dx_1x_1y_1y_1}, \frac{y_1y_1-x_1x_1}{1-dx_1x_1y_1y_1}\right).$
- No reason that the denominators should be 0.
- Addition law produces correct result also for doubling.
- Unified group operations!
- Having addition law work for doubling removes some checks from the code.

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.

Influence of inversions, Fq8 2007



Consequences

- Speed records for Diffie-Hellman key exchange.
- 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

- Speed records for Diffie-Hellman key exchange.
- 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 …
- …very important ingredient of finding relations of the form (2) for the number field sieve is the Elliptic Curve Method of factorization (ECM).
- Using Edwards curves and some new ideas we just sped up the best known ECM implementation by 7%; some more speed-up possible.
- This means that RSA got less secure while ECC got faster/more secure.

The END

Thanks!

References

- Harold M. Edwards, “A normal form for elliptic curves”, Bulletin of the AMS, **44**, 393–422, 2007. Online.
- Bernstein/L. “Faster addition and doubling on elliptic curves”, Asiacrypt 2007, pp. 29-50. Online.
- Bernstein/Birkner/L./Peters, “Optimizing double-base elliptic-curve single-scalar multiplication”, Indocrypt 2007, pp. 167–182. Online.
- Bernstein/L. “Analysis and optimization of elliptic-curve single-scalar multiplication”, Proceedings of Fq8, to appear. Online.
- Bernstein/Birkner/L./Peters, “Twisted Edwards Curves”, submitted.
- Bernstein/Birkner/L./Peters, “ECM using Edwards curves”, submitted.

Details on the blow-up

- Points with $v(u+u_4)=0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1-(4u_4^3/v_4^2)$.
- $u=-u_4$ is u-coordinate of a point iff

$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_5) \\ = \quad & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v=0$ corresponds to $(0,0)$ which maps to $(0,-1)$ on Edwards curve and to solutions of $u^2+(v_4^2/u_4^2-2u_4)u+u_4^2=0$. Discriminant is

$$(v_4^2/u_4^2-2u_4)^2-4u_4^2 = v_4^4 d,$$

  i. e., points defined over k iff d is a square.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Intuitive explanation:
The points at infinity (for which the addition law must fail) have minimal field of definition $k(\sqrt{d})$.

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and
$d x_1^2 y_1^2 (x_2^2 + y_2^2) = d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} d x_1^2 y_1^2 (x_2^2 + y_2^2) &= d x_1^2 y_1^2 + d^2 x_1^2 y_1^2 x_2^2 y_2^2 \\ &= d x_1^2 y_1^2 + \epsilon^2 \\ &= 1 + d x_1^2 y_1^2 = x_1^2 + y_1^2 \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let$(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$\begin{aligned} (x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2 \\ &= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2. \end{aligned}$$

Back to Edwards curves

$$(x_1, y_1) \oplus (x_2, y_2) = \left(\frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right)$$

What if denominators are 0?

Answer: They are never 0 if d is not a square in k.

Explicit proof: Let $(x_1, y_1), (x_2, y_2)$ be on curve, i.e., if $x_i^2 + y_i^2 = 1 + d x_i^2 y_i^2$. Write $\epsilon = d x_1 x_2 y_1 y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and $d x_1^2 y_1^2 (x_2^2 + y_2^2) = x_1^2 + y_1^2$, so

$$\begin{aligned}(x_1 + \epsilon y_1)^2 &= x_1^2 + y_1^2 + 2\epsilon x_1 y_1 = d x_1^2 y_1^2 (x_2^2 + y_2^2) + 2 x_1 y_1 d x_1 x_2 y_1 y_2 \\ &= d x_1^2 y_1^2 (x_2^2 + 2 x_2 y_2 + y_2^2) = d x_1^2 y_1^2 (x_2 + y_2)^2.\end{aligned}$$

$x_2 + y_2 \neq 0 \Rightarrow d = ((x_1 + \epsilon y_1)/x_1 y_1 (x_2 + y_2))^2 \Rightarrow d = \square$

$x_2 - y_2 \neq 0 \Rightarrow d = ((x_1 - \epsilon y_1)/x_1 y_1 (x_2 - y_2))^2 \Rightarrow d = \square$

If $x_2 + y_2 = 0$ and $x_2 - y_2 = 0$ then $x_2 = y_2 = 0$, contradiction.