Faster compact Diffie-Hellman

Craig Costello

Work in progress with Huseyin Hisil and Benjamin Smith

June 19, 2013

An elliptic curve and its (quadratic) twist

Suppose $\mathbb{F}_p = \mathbb{F}_{43}$ (-1 is non square)

$E\colon y^2 = x^3 - 3x - 1$ $\qquad$ $E'\colon -y^2 = x^3 - 3x - 1$

An elliptic curve and its (quadratic) twist

Suppose $\mathbb{F}_p = \mathbb{F}_{43}$ (-1 is non square)

$E: y^2 = x^3 - 3x - 1$ $\qquad$ $E': -y^2 = x^3 - 3x - 1$

E		E'
	$x = 0?$ $x^3 - 3x - 1 = -1$ ✗	$(0, 1), (0, -1)$
$(1, 13), (1, 30)$	$x = 1?$ $x^3 - 3x - 1 = -3$ ✓	
$(2, 1), (2, 42)$	$x = 2?$ $x^3 - 3x - 1 = 1$ ✓	
$(3, 19), (3, 24)$	$x = 3?$ $x^3 - 3x - 1 = 17$ ✓	
	$x = 4?$ $x^3 - 3x - 1 = 8$ ✗	$(4, 15), (4, 28)$
$\vdots$	$\vdots$	$\vdots$
$(42, 1), (42, 42)$	$x = 42?$ $x^3 - 3x - 1 = 1$ ✓	

An elliptic curve and its (quadratic) twist

Suppose $\mathbb{F}_p = \mathbb{F}_{43}$ (-1 is non square)

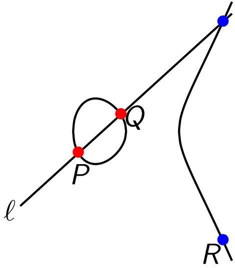
$E: y^2 = x^3 - 3x - 1$ $\qquad$ $E': -y^2 = x^3 - 3x - 1$

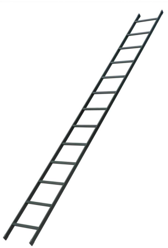
E		E'
	$x = 0?$ $x^3 - 3x - 1 = -1$ ✗	$(0,1)$, $(0,-1)$
$(1,13)$, $(1,30)$	$x = 1?$ $x^3 - 3x - 1 = -3$ ✓	
$(2,1)$, $(2,42)$	$x = 2?$ $x^3 - 3x - 1 = 1$ ✓	
$(3,19)$, $(3,24)$	$x = 3?$ $x^3 - 3x - 1 = 17$ ✓	
	$x = 4?$ $x^3 - 3x - 1 = 8$ ✗	$(4,15)$, $(4,28)$
$\vdots$	$\vdots$	$\vdots$
$(42,1)$, $(42,42)$	$x = 42?$ $x^3 - 3x - 1 = 1$ ✓	

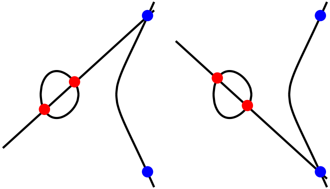
$\#E = 43 = prime \rightarrow$ ☺ $\qquad$ $\#E' = 45 = 3^2 5 \rightarrow$ ☹

Montgomery ladder for elliptic curves . . .

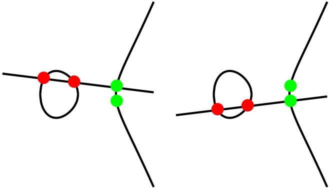
- Can compute $P + Q$ from $\{P, Q, P - Q\}$ without y-coords
- **Key:** to compute $[k]P$, have $[n+1]P$ and $[n]P$ at each stage







vs.



same difference $\rightarrow$ same result

different difference $\rightarrow$ different result

x-only needs twist-security ...

- Consider NISTp224: $p = 2^{224} - 2^{96} + 1$

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

with $b = 189582\ldots672564$

- $\#E = 2695994666715063\ldots21682722368061$ (224-bit prime)
- What about the order of the quadratic twist of NISTp224?
- $\#E' = 3^2 \cdot 11 \cdot 47 \cdot 3015283 \cdot 40375823 \cdot 267983539294927 \cdot 177594041488131583478651368420021457$ (118-bit prime)
- Not a problem if using both coordinates, just check $(x, y) \in E$
- If only dealing with x's, honest parties all work on E ☺...
  ...but attackers could take x's on E' and solve DLP there ☹
- **Solution:** Use *twist-secure* curves: $\#E$ and $\#E'$ both strong

Combining x-only with endomorphisms???

- Using Montgomery's fast/compact x-only arithmetic with endomorphisms has not been done
- **Reason 1:** GLV curves are special: twist-security (especially over best prime/s) is very unlikely
  - e.g. $y^2 = x^3 + b$ - at most 6 isomorphism classes / group orders over any prime
  - e.g. $y^2 = x^3 + ax$ - at most 4...
- **Reason 2:** GLS curves are much more plentiful, BUT (e.g. over $\mathbb{F}_{p^2}$) necessarily have insecure E'

Combining x-only with endomorphisms???

- Using Montgomery's fast/compact x-only arithmetic with endomorphisms has not been done
- **Reason 1:** GLV curves are special: twist-security (especially over best prime/s) is very unlikely
  - e.g. $y^2 = x^3 + b$ - at most 6 isomorphism classes / group orders over any prime
  - e.g. $y^2 = x^3 + ax$ - at most 4...
- **Reason 2:** GLS curves are much more plentiful, BUT (e.g. over $\mathbb{F}_{p^2}$) necessarily have insecure E'
- **NEWSFLASH**: **Smith'2013/312** gives twist-secure construction with many curves over any particular field
  - $\mathbb{Q}$-curves: curves over quadratic number field with isogeny to their Galois conjugate
  - $\approx p$ pairs of (E, E') over $\mathbb{F}_{p^2}$
  - 2-dimensional decomposition possible
  - **more news**: he's coming in August, so details in his talk

2GLV using ϕ... having (x, y) vs. having x-only

Reason 3:

- To compute $[k]P$ from P

  $k = [1,0,0,1,1,1,0,1,0,\ldots,1,1,0,0,0,0,1,0,1]$ (256 bits)

- Suppose $\phi(P) = Q$, so $[k]P = [k_0]P + [k_1]Q$

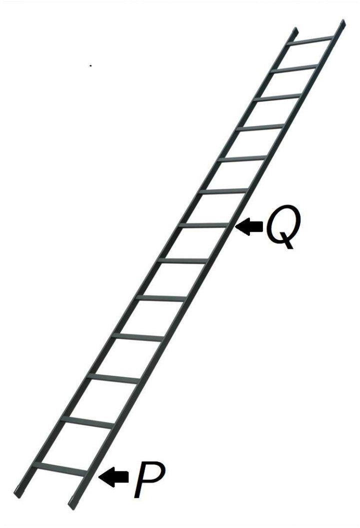
  $k_0 = [0,1,0,0,\ldots 0,1,0,1]$ (128 bits)
  $k_1 = [1,1,1,0,\ldots 1,1,0,0]$ (128 bits)

- Usual approach fine when we have (x, y) and can perform add P and Q immediately or add whatever/whenever we like

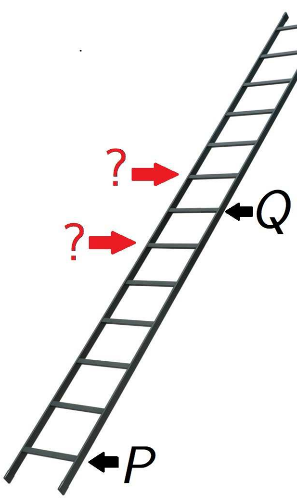
- **BUT:** can't add (in Montgomery land) with x-only

- Can't move anywhere with just P and Q

Can't move anywhere with just P and Q...



Need $Q - P$ or $Q + P$ to move quickly to $[k]P$



Computing $(\phi - 1)(P)$ and $(\phi + 1)(P)$

- Smith: Hasegawa $\mathbb{Q}$-curves of degree 2 over $\mathbb{F}_{p^2}$
- $\phi(x, y) = (x', y')$ on the Weierstrass model, given as

$$(x', y') = \left(\frac{-x^p}{2} - \frac{c^p}{x^p - 4} \quad , \quad \frac{y^p}{\sqrt{-2}} \left(\frac{-1}{2} + \frac{c^p}{(x^p-4)^2} \right) \right)$$

  for some curve constant c
- Write x-coordinate, x^+, of $\phi(P) + P$ explicitly

$$\begin{aligned} x^+ = \lambda^2 - x - x' &= \left(\frac{y' - y}{x' - x} \right)^2 - x - x' \\ &= \left(\frac{y^p \cdot f(x) - y}{x' - x} \right)^2 - x - x' \\ &= \left(\frac{(y^2)^p - 2f(x) y^{p+1} + y^2}{(x' - x)^2} \right) - x - x' \end{aligned}$$

- the y^2 terms go away, it's just y^{p+1} that is left ...

Computing $(\phi - 1)(P)$ and $(\phi + 1)(P)$

- How to deal with y^{p+1}: p is odd, so

$$\begin{aligned} y^{p+1} &= (y^2)^{(p+1)/2} \\ &= (x^3 + ax + b)^{(p+1)/2} \end{aligned}$$

- Still a fairly undesirable exponentiation in general, **BUT** ...

Computing $(\phi - 1)(P)$ and $(\phi + 1)(P)$

- How to deal with y^{p+1}: p is odd, so

$$\begin{aligned} y^{p+1} &= (y^2)^{(p+1)/2} \\ &= (x^3 + ax + b)^{(p+1)/2} \end{aligned}$$

- Still a fairly undesirable exponentiation in general, **BUT** ...
- Let's target 128-bit security, and take $E/\mathbb{F}_{p^2}$ with

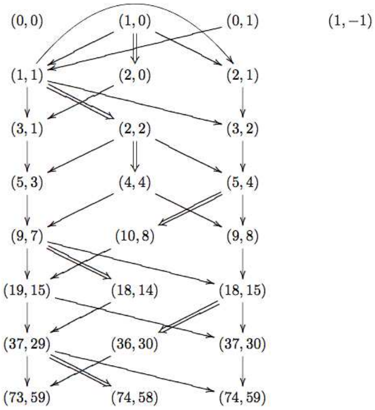
$$p = 2^{127} - 1$$

- Exponent is now 2^{126}, i.e. requires 126 repeated squarings
- Squarings much cheaper than multiplications in $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$
- Translation to Montgomery form is immediate

...maybe not so bad after all ...

Two dimensional differential addition chains...

- To compute $[m]P + [n]Q$ 'differentially', Bernstein proposed fast constant-time chain



- 1 DBL + 2 ADD per bit of $\log_2(\max(m, n))$

How fast are we talking?

- Compare to Bernstein's `curve25519` (best x-only):

  255 montDBL + 255 montADD

- $\mathbb{Q}$-curve over $\mathbb{F}_{p^2}$ with $p = 2^{127} - 1$:

  ϕ cost + 127 montDBL + 254 montADD

- ϕ costs a little more than 126 squarings, but we save as many montDBL's (2 mults + 2 squarings each)

- **bonus:** we work over Mersenne quadratic extension, fast modular (lazy) reduction

...timings (and much more) to come ...

Some questions to be answered ...

1. can non-constant time addition chains (with half as many ops per bit - e.g. Peter's PRAC) rival the non-resistant records?
2. can we avoid decomposition and simply start with k_0 and k_1?
3. is it possible to do better in computing $\phi \pm 1$ explicitly?
4. how to make things *truly* constant-time?
5. what more can we do when we know the point (coordinate) x_P in advance (i.e. fixed base scenario)?
6. $\phi \pm 1$ maps on the genus 2 Kummers: not giving up yet ☹...