# FourQ

Four-dimensional decompositions on a $\mathbb{Q}$-curve

Joint work with Patrick Longa

http://research.microsoft.com/pubs/246916/main.pdf

*"NIST should generate a new set of elliptic curves [...] and should incorporate the latest knowledge..."*

[Edward Felten, VCAT document, page 9].

*"NIST should generate a new set of elliptic curves [...] and should incorporate the latest knowledge..."*

[Edward Felten, VCAT document, page 9].

## Some 21st century ECC milestones

**2001:** CM endomorphisms [GLV01]

**2007:** Edwards curves [Edw07,BL07]

**2008:** Twisted Edwards coordinates [BBJ+08,HCWD08]

**2009:** Frobenius endomorphisms [GLS09]

**2013:** Q-curve endomorphisms [Smi13]

*"NIST should generate a new set of elliptic curves [...] and should incorporate the latest knowledge..."*

[Edward Felten, VCAT document, page 9].

## Some 21st century ECC milestones

2001: CM endomorphisms [GLV01]

2007: Edwards curves [Edw07,BL07]

2008: Twisted Edwards coordinates [BBJ+08,HCWD08]

2009: Frobenius endomorphisms [GLS09]

2013: Q-curve endomorphisms [Smi13]

→ **Four**$\mathbb{Q}$

*"I don't care about a performance difference unless it is at least a factor of two."*

[Phillip Hallam-Baker, CFRG mailing list, 12 Mar 2015, 3 Feb 2015,...].

*"I don't care about a performance difference unless it is at least a factor of two."*

[Phillip Hallam-Baker, CFRG mailing list, 12 Mar 2015, 3 Feb 2015,...].

$$\frac{\#\text{cycles(NUMS,curve25519,etc)}}{\#\text{cycles}(\mathbf{Four}\mathbb{Q})} \gg 2.5$$

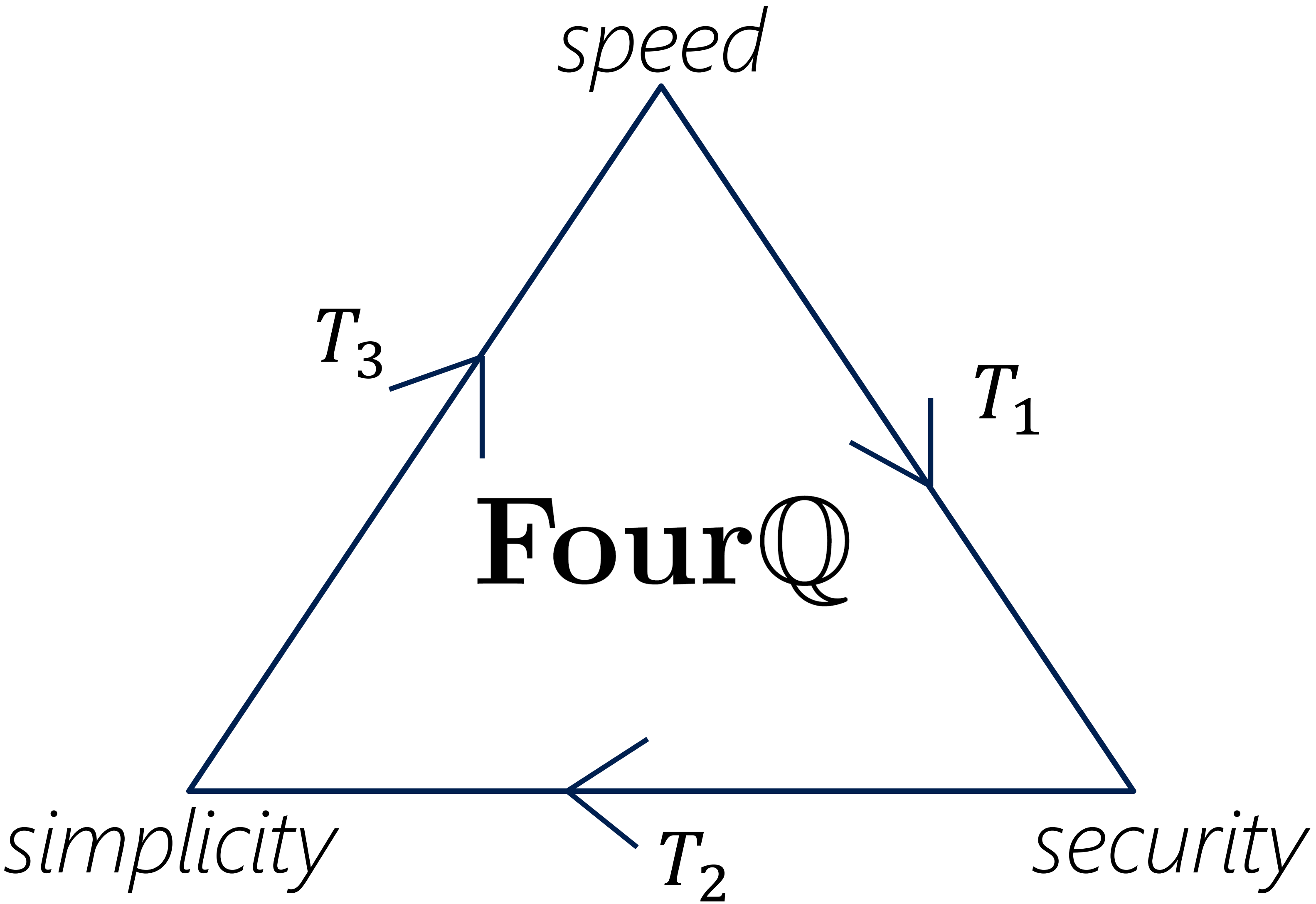
$$\frac{\#\text{cycles(NIST Curvep256)}}{\#\text{cycles}(\mathbf{Four}\mathbb{Q})} \gg 4.5$$

*“Minimize tensions between speed, simplicity, & security.”*

[Daniel J. Bernstein, CFRG mailing list, 1 Aug 2014, 21 Nov 2014, …].

*"Minimize tensions between speed, simplicity, & security."*

[Daniel J. Bernstein, CFRG mailing list, 1 Aug 2014, 21 Nov 2014, ...].




$$\sum_{i=1}^{3} T_i = 0$$

# The curve

$$E/\mathbb{F}_{p^2}\colon -x^2 + y^2 = 1 + dx^2y^2,$$

$$d = 125317048443780598345676279555970305165 \cdot i \quad + \quad 4205857648805777768770$$

$$\#E = 392 \cdot N\,, \quad \text{where } N \text{ is a 246-bit prime}$$

# The curve

$$E/\mathbb{F}_{p^2}: -x^2 + y^2 = 1 + dx^2y^2,$$

$$d = 125317048443780598345676279555970305165 \cdot i \quad + \quad 4205857648805777768770$$

$$\#E = 392 \cdot N\,,$$ where $N$ is a 246-bit prime

- Fastest (large char) ECC addition laws are *complete* on $E$
- $E$ is a degree-2 Q-curve: endomorphism $\psi$
- $E$ has CM by order of $D = -40$: endomorphism $\phi$
- $\psi(P) = [\lambda_\psi]P$ and $\phi(P) = [\lambda_\phi]P$ for all $P \in E[N]$ and $m \in [0, 2^{256})$

$$m \mapsto (a_1, a_2, a_3, a_4)$$

$$[m]P = [a_1]P + [a_2]\phi(P) + [a_3]\psi(P) + [a_4]\psi(\phi(P))$$

# Security aspects

- Pollard rho best attack on ECDLP: $\mathbf{2^{122.5}}$ additions in $\boldsymbol{E[N]}$

# Security aspects

- Pollard rho best attack on ECDLP: $2^{122.5}$ additions in $E[N]$

- Unlike typical GLV and GLS endomorphisms, no speedup in rho from $\psi$ and $\phi$

# Security aspects

- Pollard rho best attack on ECDLP: $\mathbf{2^{122.5}}$ additions in $E[N]$
- Unlike typical GLV and GLS endomorphisms, no speedup in rho from $\boldsymbol{\psi}$ and $\boldsymbol{\phi}$
- $\mathbb{F}_{p^2}$ safe against index calculus/Weil descent

# Security aspects

- Pollard rho best attack on ECDLP: $2^{122.5}$ additions in $E[N]$
- Unlike typical GLV and GLS endomorphisms, no speedup in rho from $\psi$ and $\phi$
- $\mathbb{F}_{p^2}$ safe against index calculus/Weil descent
- Large MOV degree and trace of Frobenius

# Security aspects

- Pollard rho best attack on ECDLP: $2^{122.5}$ additions in $E[N]$
- Unlike typical GLV and GLS endomorphisms, no speedup in rho from $\psi$ and $\phi$
- $\mathbb{F}_{p^2}$ safe against index calculus/Weil descent
- Large MOV degree and trace of Frobenius
- Yes, small discriminant ($D = -40$), just like other standardized curves $secp192k1$, $secp224k1$, $secp256k1$ (Bitcoin's curve)

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0, 2^{256})$, *decomposition yields four* $a_i \in [1, 2^{64})$ *with* $a_1$ *odd.*

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0,2^{256})$*, decomposition yields four* $a_i \in [1,2^{64})$ *with* $a_1$ *odd.*

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515378 8

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0, 2^{256})$, *decomposition yields four* $a_i \in [1, 2^{64})$ *with* $a_1$ *odd.*

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515378 8

$a_1 = 1444512474917004704 1$

$a_2 = 1163837646117911507 5$

$a_3 = 503291171168028635 8$

$a_4 = 88109258282884243 1$

$a_1 =$ 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1 $\quad P$

$a_2 =$ 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 $\quad \phi(P)$

$a_3 =$ 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 $\quad \psi(P)$

$a_4 =$ 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0 $\quad \phi(\psi(P))$

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0,2^{256})$, *decomposition yields four* $a_i \in [1,2^{64})$ *with* $a_1$ *odd.*

$m$ = 64840569332679984426672436340494668739430332089137885001096300239355695153788

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

$a_1$ = 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1 — $P$
$a_2$ = 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 — $\phi(P)$
$a_3$ = 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 — $\psi(P)$
$a_4$ = 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0 — $\phi(\psi(P))$

do nothings can leak info!

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all $m \in [0, 2^{256})$, decomposition yields four $a_i \in [1, 2^{64})$ with $a_1$ odd.*

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515378

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

$a_1$ = 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1    $P$
$a_2$ = 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1    $\phi(P)$
$a_3$ = 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0    $\psi(P)$
$a_4$ = 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0    $\phi(\psi(P))$

$0, 1$ ⟷ $1, -1$

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0, 2^{256})$*, decomposition yields four* $a_i \in [1, 2^{64})$ *with* $a_1$ *odd.*

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515378

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

$a_1$ = 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0 0, 1, -1 $\quad P$
$a_2$ = 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 $\quad \phi(P)$
$a_3$ = 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 $\quad \psi(P)$
$a_4$ = 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0 $\quad \phi(\psi(P))$

$0, 1 \longleftrightarrow 1, -1$

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0,2^{256})$, *decomposition yields four* $a_i \in [1,2^{64})$ *with* $a_1$ *odd.*

$m$ = 64840569332679984426672436340494668739430332089137885001096300239355695153788

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

$a_1$ = 1,-1,1,1,-1,-1,1,-1,-1,-1,-1,1, 1, 1,-1, 1, 1, 1,-1,1,1,-1,-1,1,-1,-1,-1, 1, 1,-1, 1, 1,-1, 1,-1,-1,-1,-1,-1,-1,1,-1,-1, 1,1,1, 1,-1, 1 ,1,1,1,1,1,1,-1,-1,-1,-1, 1,-1,-1,-1, 1,-1 $P$
$a_2$ = 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 $\phi(P)$
$a_3$ = 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 $\psi(P)$
$a_4$ = 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0 $\phi(\psi(P))$

$0, 1$ ⟷ $1, -1$

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5:** *for all* $m \in [0, 2^{256})$, *decomposition yields four* $a_i \in [1, 2^{64})$ *with* $a_1$ *odd*.

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515378 8

$a_1$ = 14445124749170047041
$a_2$ = 11638376461179115075
$a_3$ = 5032911711680286358
$a_4$ = 881092582828842431

$a_1$ = 1,-1,1,1,-1,-1,1,-1,-1,-1,-1,1, 1, 1,-1, 1, 1, 1,-1,1,1,-1,-1,1,-1,-1,-1, 1, 1,-1, 1, 1,-1, 1,-1,-1,-1,-1,-1,-1,1,-1,-1, 1,1,1, 1,-1, 1 ,1,1,1,1,1,1,-1,-1,-1,-1, 1,-1,-1,-1, 1,-1 $P$
$a_2$ = 0, 1, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1 $\phi(P)$
$a_3$ = 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0 $\psi(P)$
$a_4$ = 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0 $\psi(\phi(P))$

- All columns now non-zero
- Could stop here, but we can do better!
- Lookup table currently size 16, but we turn it into size 8: "sign-align" three bottom rows with top one
- All of this is done in constant time… and…

# Optimal Scalar Decompositions

$$m \mapsto (a_1, a_2, a_3, a_4)$$

**Prop 5 + Prop 6:** *for all* $m \in [0, 2^{256})$*, decomposition yields* $s = \{-1,1\}^{65}$ *and* $d = [1,8]^{65}$

$m$ = 6484056933267998442667243634049466873943033208913788500109630023935569515 3788

$s_i =$ -1,-1,-1,-1,-1, 1,-1,-1,-1,-1, 1, 1, 1, 1, 1, 1, 1,-1, 1, 1, 1, 1,-1,-1, 1,-1,-1,-1,-1,-1,-1, 1,-1, 1, 1,-1, 1, 1,-1,-1,-1, 1,-1,-1, 1, 1,-1, 1, 1, 1,-1, 1, 1, 1,-1,-1,-1,-1, 1,-1,-1, 1, 1,-1, 1

$d_i =$ 2, 7, 6, 4, 2, 4, 2, 8, 4, 5, 5, 6, 4, 5, 4, 1, 4, 7, 7, 4, 8, 5, 6, 7, 4, 6, 6, 3, 8, 8, 2, 3, 4, 3, 6, 8, 3, 5, 6, 7, 7, 2, 5, 5, 2, 1, 6, 3, 5, 5, 6, 8, 3, 1, 7, 6, 5, 4, 6, 7, 3, 4, 3, 6, 6

$$T[1] = P$$
$$T[2] = P + \phi(P)$$
$$\ldots$$
$$T[8] = P + \phi(P) + \psi(P) + \psi(\phi(P))$$

# The full routine

- On input of any $P \in E[N]$ and any $m \in [0, 2^{256})$, do:

1. Compute endomorphisms $P \mapsto \phi(P), \psi(P), \psi(\phi(P))$ — $68\,\boldsymbol{M} + 27\boldsymbol{S} + 49.5\boldsymbol{A}$
2. Decompose $m \mapsto (a_1, a_2, a_3, a_4)$
3. Recode $(a_1, a_2, a_3, a_4) \mapsto d, s$
4. Compute table $[P, \ldots, P + \phi(P) + \psi(P) + \psi(\phi(P))]$ — $68\,\boldsymbol{M} + 66\boldsymbol{A}$
5. Execute main loop (64 complete DBL-ADD steps) — $768\,\boldsymbol{M} + 192\boldsymbol{S} + 771\boldsymbol{A}$
6. Normalize and return — $1\boldsymbol{I} + 2\,\boldsymbol{M}$

- Theorem 1: computes correctly in: $1\boldsymbol{I} + 906\,\boldsymbol{M} + 219\boldsymbol{S} + 886.5\boldsymbol{A}$
- Our constant time imp: 73,000cc (Ivy) 76,000cc (Sandy)

# Cofactor killing

- As with all composite order curves, some cryptographic scalar multiplications must avoid subgroup attacks
- We compute $P \mapsto [392]P$ in the naïve way (8 DBLs, 2ADDs) beforehand (and are still significantly faster than all other primitives)
- Can absorb part of the cofactor into the decomposition for free, but we keep it simple!

# Other high-speed contenders?


- g=2 Kummer efficiency currently restricted to DH, i.e., can't do Schnorr-style signatures, precomputation for fast ECDHE or more versatile crypto ☹
- And well, binary GLS uses a binary curve ☹

# "**Four**$\mathbb{Q}$, I won't do what you tell me!"

- If you don't want to use endomorphisms, you don't have to: naïve scalar multiplication will still be faster because this field is the fastest
- If you don't want to use twisted Edwards coordinates, then don't: Weierstrass version still fast! Heck, do Montgomery if you want
- **Four**$\mathbb{Q}$ is very versatile!

# Summary

- The demand for high-performance cryptography warrants the state-of-the-art in ECC to be part of the standardization discussion
- This work shows the performance gains that are possible if such a curve were to be standardized alongside the “conservative” choices

# References

[GLV01] R. P. Gallant, R. J. Lambert, S. A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. CRYPTO 2001: 190-200.

[Edw07] H. Edwards. A normal form for elliptic curves. Bulletin of the AMS, 44:3. 2007. 393-422.

[BL07] D. J. Bernstein and T. Lange. Faster Addition and Doubling on Elliptic Curves. ASIACRYPT 2007: 29-50.

[BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters. Twisted Edwards curves. AFRICACRYPT 2008: 389-405.

[HCWD08] H. Hisil, G. Carter, K. K. Wong, E. Dawson. Twisted Edwards curves revisited. ASIACRYPT 2008: 326-343.

[GLS09] S. D. Galbraith, X. Lin, M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. EUROCRYPT 2009: 518-535.

[Smi13] B. Smith. Fast families of elliptic curves from Q-curves. ASIACRYPT 2013: 61-78

[VCAT] Report and Recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

[CFRG] Crypto Forum Research Group Discussion Archive: http://www.ietf.org/mail-archive/web/cfrg/current/maillist.html

# FourQ

Joint work with Patrick Longa

http://research.microsoft.com/pubs/246916/main.pdf