# (Genus) 2 > (Genus) 1

Joppe W. Bos

Microsoft Research

Joint work with Craig Costello, Huseyin Hisil and Kristin Lauter

Microsoft Research

YASAR UNIVERSITY

# Motivation

Elliptic (genus-1) curve cryptography is a standardized approach to instantiate public-key cryptography

The current standards are reasonably fast

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| NISTp-256 [3] | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |

[3] OpenSSL 1.0.1

# Motivation

Elliptic (genus-1) curve cryptography is a standardized approach to instantiate public-key cryptography

The current standards are reasonably fast

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 [1] | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV [2] | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 [3] | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |

[1] D. J. Bernstein. Curve25519: New Diffie-Hellman speed records. PKC 2006
[2] P. Longa and F. Sica. Four-dimensional Gallant-Lambert-Vanstone scalar multiplication. Asiacrypt 2012
[3] OpenSSL 1.0.1

# Motivation

Elliptic (genus-1) curve cryptography is a standardized approach to instantiate public-key cryptography

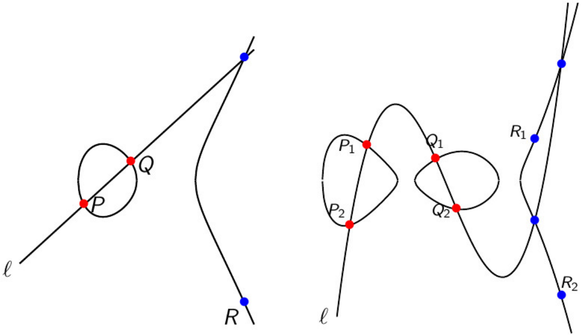
The current standards are reasonably fast

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 [1] | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV [2] | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 [3] | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |

- People have studied Jacobians of hyperelliptic curves (genus $g > 1$) curves in crypto
- This is considered insecure for $g > 2$
- What about $g == 2$?

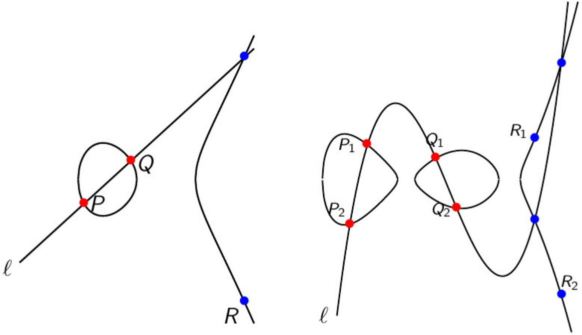

[1] D. J. Bernstein. Curve25519: New Diffie-Hellman speed records. PKC 2006
[2] P. Longa and F. Sica. Four-dimensional Gallant-Lambert-Vanstone scalar multiplication. Asiacrypt 2012
[3] OpenSSL 1.0.1

# Genus 2: why bother?




**Disadvantage 1:** Point counting

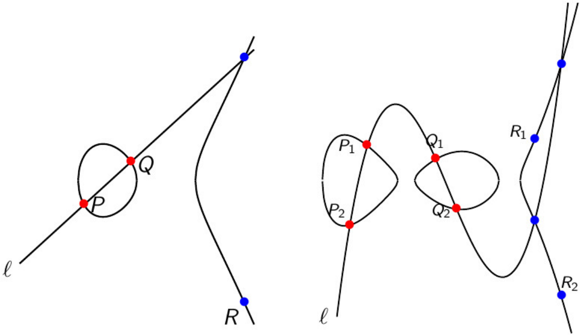
# Genus 2: why bother?




Generic methods for genus-2 point counting have become practical

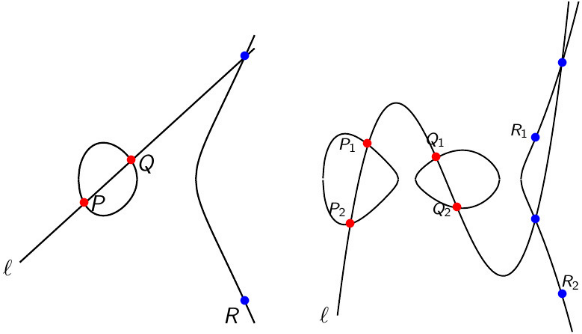
P. Gaudry and É. Schost. Genus 2 point counting over prime fields. J. Symb. Comput. 2012

# Genus 2: why bother?




**Disadvantage 2:** Group Law

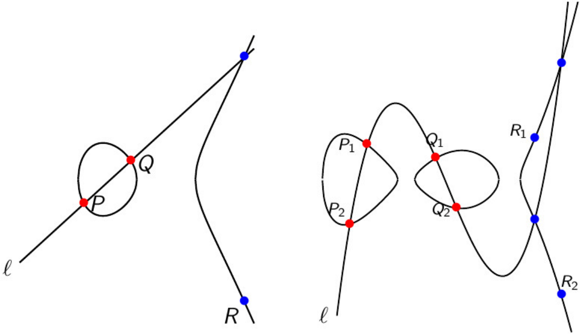
# Genus 2: why bother?




Elliptic: $E : y^2 = x^3 + \dots$ Hyperelliptic: $C : y^2 = x^5 + \dots$

- $\#E(\mathbb{F}_p) \approx \#\mathrm{Jac}(C(\mathbb{F}_q))$ for $q^2 \approx p$
- Elliptic curve 256-bit arithmetic **versus** genus-2 128-bit arithmetic

# Genus 2: why bother?

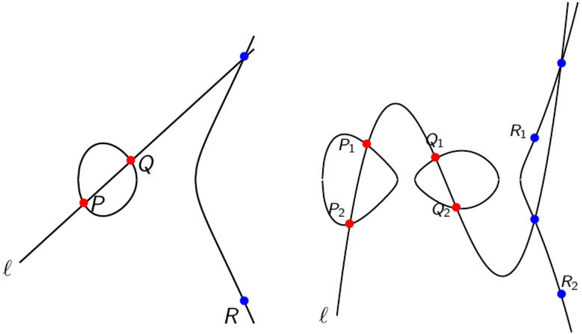



per bit: $\approx$ **10** $\times$ 256-bit muls vs. $\approx$ **50** $\times$ 128-bit muls

- unfortunately: $1 \times$ 256-bit mul $< 5 \times$ 128-bit mul

C. Costello and K. Lauter. Group law computations on Jacobians of hyperelliptic curves. SAC 2011

# Genus 2: why bother?




per bit: $\approx$ **10** $\times$ 256-bit muls vs. $\approx$ **50** $\times$ 128-bit muls

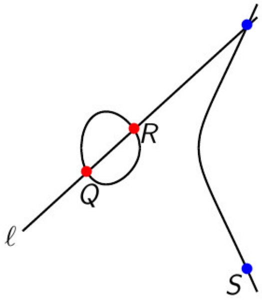
- unfortunately: $1 \times$ 256-bit mul $< 5 \times$ 128-bit mul
- But genus-1 estimate uses all the known tricks (genus-2's doesn't)

C. Costello and K. Lauter. Group law computations on Jacobians of hyperelliptic curves. SAC 2011

# 1. The Kummer surface

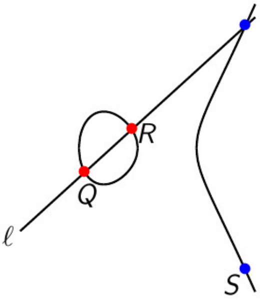
# A wise man once said. . .

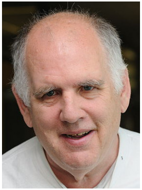
**Who needs the $y$-coordinate?**



# A wise man once said. . .

**Who needs the *y*-coordinate?**



- Don't use $(Q_x, Q_y)$ and $(R_x, R_y)$ to get $(S_x, S_y)$
- Instead, use $Q_x, R_x, (Q - R)_x$ to get $(Q + R)_x$
- Enough to define scalar multiplication: Montgomery ladder
- To compute $[k]P$, always keep $Q = [n + 1]P$, $R = [n]P$, so we have $Q - R = P$

# The genus 2 analogue: the Kummer surface $\mathcal{K}$

- For $P = (x_P, y_P)$, Montgomery took $P \mapsto P_x$ (two-to-one)

- There is a map $\mathrm{Jac}(C) \to \mathcal{K}$ that is two-to-one

$$\mathcal{K}: \quad (x^4 + y^4 + z^4 + t^4) + 2Exyzt - F(x^2t^2 + y^2z^2) - G(x^2z^2 + y^2t^2) - H(x^2y^2 + z^2t^2) = 0$$

- We lose information, but on the other hand can enjoy beautiful symmetries that exist on $\mathcal{K}$...

# The genus 2 analogue: the Kummer surface $\mathcal{K}$

- e.g. to get from $P=(x,y,z,t)$, $Q=(\underline{x},\underline{y},\underline{z},\underline{t})$, $P-Q=(\overline{x},\overline{y},\overline{z},\overline{t})$ to $P+Q=(X,Y,Z,T)$

$$
\begin{aligned}
x' &= (x^2+y^2+z^2+t^2)\cdot(\underline{x}^2+\underline{y}^2+\underline{z}^2+\underline{t}^2)\\
y' &= (x^2+y^2-z^2-t^2)\cdot(\underline{x}^2+\underline{y}^2-\underline{z}^2-\underline{t}^2)\\
z' &= (x^2-y^2+z^2-t^2)\cdot(\underline{x}^2-\underline{y}^2+\underline{z}^2-\underline{t}^2)\\
t' &= (x^2-y^2-z^2+t^2)\cdot(\underline{x}^2-\underline{y}^2-\underline{z}^2+\underline{t}^2)\\
X &= (x'^2+y'^2+z'^2+t'^2)/\overline{x}\\
Y &= (x'^2+y'^2-z'^2-t'^2)/\overline{y}\\
Z &= (x'^2-y'^2+z'^2-t'^2)/\overline{z}\\
T &= (x'^2-y'^2-z'^2+t'^2)/\overline{t}
\end{aligned}
$$

- $\mathcal{K}$ not a group, but "pseudo-group" - enough to define scalar multiplications via ladder (and do Diffie-Hellman)
- Total per bit (DBL+ADD) of scalar: **25 $\times$ $\mathbb{F}_p$ multiplications!**

D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Advances in Applied Mathematics, 1986.
N. P. Smart and S. Siksek. A fast Diffie-Hellman protocol in genus 2. Journal of Cryptology, 1999.
P. Gaudry. Fast genus 2 arithmetic based on theta functions. Journal of Mathematical Cryptology, 2007.

# 2. GLV scalar decomposition

R. P. Gallant, R. J. Lambert, and S. A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. CRYPTO 2001.

# 2. GLV scalar decomposition

**$d$-dimensional GLV**

Decompose a $k$-bit scalar in $d$ "mini-scalars" of bit-length $O(\sqrt[d]{k})$

R. P. Gallant, R. J. Lambert, and S. A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. CRYPTO 2001.

# GLV: e.g. Buhler-Koblitz curves

- Let $p = 1 + 2^{64} - 2^{66} + 2^{68} - 2^{70} + 2^{72} + 2^{74} + 2^{76} - 2^{79} + 2^{127}$
- Consider the prime order (254-bit) Buhler-Koblitz curve:
  $$C/\mathbb{F}_p : y^2 = x^5 + 17$$
- There is a map on $C$ , $\phi : (x, y) \mapsto (\xi_5 x, y)$ where $\xi_5^5 = 1$
- It induces a map on $\mathrm{Jac}(C)$ (Mumford coordinates):
  $$\phi : (u_1, u_0, v_1, v_0) \mapsto (\xi_5 u_1, \xi_5^2 u_0, \xi_5^4 v_1, v_0)$$
- For $D \in \mathrm{Jac}(C)$, $\phi(D)$ is a scalar multiple $[\lambda]D$ of $D$
- Minimal polynomial $\phi^4 + \phi^3 + \phi^2 + \phi + 1$, so $\phi^2(D)$ and $\phi^3(D)$ will also be useful

# GLV: e.g. Buhler-Koblitz curves

- Take a random $D = (u_1, u_0, v_1, v_0)$, assume we have to compute the scalar multiplication by
  $k = 2347739983727893692359949371328647095531478579834751919719957812025908901668\,0$
- The endomorphism $\phi$ corresponds to multiplication by
  $\lambda = 7831546867685512705297615980651794586753229241310765320406147783708756285646$
- So (essentially) for free we get

$$D, \qquad \phi(D) = [\lambda]D, \qquad \phi^2(D) = [\lambda^2]D, \qquad \phi^3(D) = [\lambda^3]D$$

- How best to combine the 4 scalar multiples?...find the minimum $k_0, k_1, k_2, k_3$ such that

$$[k]D = [k_0]D + [k_1]\phi(D) + [k_2]\phi^2(D) + [k_3]\phi^3(D)$$

# GLV: e.g. Buhler-Koblitz curves

- $k = 2347739983727893692359949371328647095531478579834751919719957812025908901668 0$
- Finding $k_0, k_1, k_2, k_3$ s.t.
  $[k]D = [k_0]D + [k_1]\phi(D) + [k_2]\phi^2(D) + [k_3]\phi^3(D)$
  involves solving a shortest-vector problem
- We use algorithm from [1], so that in $\approx 20 \times \mathbb{F}_p$ muls, we get

$$
\begin{aligned}
k_0 &= -6344646642321980551 \quad \text{(63 bits)} \\
k_1 &= -3170471730617986668 \quad \text{(62 bits)} \\
k_2 &= -4387949940648063094 \quad \text{(62 bits)} \\
k_3 &= 3721725683392112311 \quad \text{(62 bits)}
\end{aligned}
$$

- How to proceed?

[1] Y.-H. Park, S. Jeong, and J. Lim. Speeding up point multiplication on hyperelliptic curves with efficientlycomputable endomorphisms. Eurocrypt 2002

# GLV - Arithmetic

Non-GLV: $253\mathbf{D} + \approx 23\mathbf{A}$

$$[k]D = [k_0]D + [k_1]\phi(D) + [k_2]\phi^2(D) + [k_3]\phi^3(D)$$

# GLV - Arithmetic

Non-GLV: $253\mathbf{D}+ \approx 23\mathbf{A}$

$$[k]D = [k_0]D + [k_1]\phi(D) + [k_2]\phi^2(D) + [k_3]\phi^3(D)$$

## Approach 1 - Vertical slices

Precompute for $0 \leq i < 2^4$: $L_i = \sum_{\ell=0}^{3} \left[ \left\lfloor \frac{i}{2^\ell} \right\rfloor \bmod 2 \right] \phi^\ell(D)$

$j$th bit: Add $L_i$ for $i = \sum_{\ell=0}^{d-1} 2^\ell \left( \left\lfloor \frac{k_\ell}{2^j} \right\rfloor \bmod 2 \right)$

Cost: $\leq (62\mathbf{A} + 62\mathbf{D}) + (11\mathbf{A} + 3\mathbf{D})$

# GLV - Arithmetic

Non-GLV: $253\mathbf{D} + \approx 23\mathbf{A}$

$$[k]D = [k_0]D + [k_1]\phi(D) + [k_2]\phi^2(D) + [k_3]\phi^3(D)$$

## Approach 1 - Vertical slices

Precompute for $0 \leq i < 2^4$: $L_i = \sum_{\ell=0}^{3} \left[ \left\lfloor \frac{i}{2^\ell} \right\rfloor \bmod 2 \right] \phi^\ell(D)$

$j$th bit: Add $L_i$ for $i = \sum_{\ell=0}^{d-1} 2^\ell \left( \left\lfloor \frac{k_\ell}{2^j} \right\rfloor \bmod 2 \right)$

Cost: $\leq (62\mathbf{A} + 62\mathbf{D}) + (11\mathbf{A} + 3\mathbf{D})$

## Approach 2 - Individual windowing

$d$ lookup tables: $L_\ell(c) = [c]P_\ell$

$j$th part: $\sum_{\ell=0}^{d-1} \pm L_\ell( \left\lfloor \frac{k_\ell}{2^{wj}} \right\rfloor \bmod 2^w)$

Use $\phi$ to get the other $(d-1)$ lookup tables, cost $= \delta$.

4-bit signed windows, precomp: $8\mathbf{D} + 7\mathbf{A}$

Cost: $\approx 62\mathbf{D} + \lceil 63/5 - 1 \rceil (1+3)\mathbf{A} + \delta = 62\mathbf{D} + 48\mathbf{A} + \delta$

# Special primes I

- Practical point counting for genus-2
- Kummer surface, GLV decomposition
- Let's try to find some primes which allow fast reduction.

### NIST-like reduction

For instance primes of the form: $2^s - c$ with $0 \leq c < 2^{64}$.
Example: $s = 127$, $c = 1$. Let $0 \leq a, b < 2^{127} - 1$
$c = a \cdot b = c_1 \cdot 2^{128} + c_0$ for $0 \leq c_1, c_0 < 2^{128}$.

# Special primes I

- Practical point counting for genus-2
- Kummer surface, GLV decomposition
- Let's try to find some primes which allow fast reduction.

### NIST-like reduction

For instance primes of the form: $2^s - c$ with $0 \leq c < 2^{64}$.
Example: $s = 127$, $c = 1$. Let $0 \leq a, b < 2^{127} - 1$
$c = a \cdot b = c_1 \cdot 2^{128} + c_0$ for $0 \leq c_1, c_0 < 2^{128}$.
$c' = (c_0 \bmod 2^{127}) + 2 \cdot c_1 + \lfloor c_0/2^{127} \rfloor \equiv c \bmod 2^{127} - 1$
Now $0 \leq c' < 2^{128}$. Reduction requires no multiplications.

**Input:**

$$\begin{cases} A = \sum_{i=0}^{n-1} a_i r^i, B, p, \mu \text{ such that} \\ 0 \leq a_i < r,\ 0 \leq A, B < r^n, \\ r^{n-1} \leq p < r^n, 2 \nmid p, \\ \gcd(r, p) = 1,\ \mu = -p^{-1} \bmod r, \end{cases}$$

**Output:** $\begin{cases} C \equiv A \cdot B \cdot r^{-n} \bmod p \\ \text{such that } 0 \leq C < r^n \end{cases}$

$C \leftarrow 0$
**for** $i = 0$ to $n - 1$ **do**
  $C \leftarrow C + a_i \cdot B$
  $q \leftarrow \mu \cdot C \bmod r$
  $C \leftarrow (C + q \cdot p)/r$
**end for**
**if** $C \geq r^n$ **then**
  $C \leftarrow C - p$
**end if**
**return** $C$

# Special primes II - Montgomery friendly primes

**Input:** $\begin{cases} A = \sum_{i=0}^{n-1} a_i r^i, B, p, \mu \text{ such that} \\ 0 \le a_i < r,\ 0 \le A, B < r^n, \\ r^{n-1} \le p < r^n, 2 \nmid p, \\ \gcd(r, p) = 1,\ \mu = -p^{-1} \bmod r, \end{cases}$

**Output:** $\begin{cases} C \equiv A \cdot B \cdot r^{-n} \bmod p \\ \text{such that } 0 \le C < r^n \end{cases}$

1: $C \leftarrow 0$
2: **for** $i = 0$ to $n - 1$ **do**
3: $\quad C \leftarrow C + a_i \cdot B$
4: $\quad q \leftarrow \mu \cdot C \bmod r$
5: $\quad C \leftarrow (C + q \cdot p)/r$
6: **end for**
7: **if** $C \ge r^n$ **then**
8: $\quad C \leftarrow C - p$
9: **end if**
10: **return** $C$

- Let $\mu = -p^{-1} \bmod r = \pm 1$


A. K. Lenstra. Generating RSA moduli with a predetermined portion. Asiacrypt 1998
M. Knežević, F. Vercauteren, and I. Verbauwhede. Speeding up bipartite modular multiplication.WAIFI 2010
T. Acar and D. Shumow. Modular reduction without pre-computation for special moduli. Microsoft Research, 2010
M. Hamburg. Fast and compact elliptic-curve cryptography. Cryptology ePrint Archive, Report 2012/309

# Special primes II - Montgomery friendly primes

**Input:**

$$\begin{cases} A = \sum_{i=0}^{n-1} a_i r^i, B, p, \mu \text{ such that} \\ 0 \le a_i < r,\ 0 \le A, B < r^n, \\ r^{n-1} \le p < r^n, 2 \nmid p, \\ \gcd(r,p) = 1,\ \mu = -p^{-1} \bmod r, \end{cases}$$

**Output:** $\begin{cases} C \equiv A \cdot B \cdot r^{-n} \bmod p \\ \text{such that } 0 \le C < r^n \end{cases}$

1: $C \leftarrow 0$
2: **for** $i = 0$ to $n-1$ **do**
3: $C \leftarrow C + a_i \cdot B$
4: $q \leftarrow \mu \cdot C \bmod r$
5: $C \leftarrow (C + q \cdot p)/r$
6: **end for**
7: **if** $C \ge r^n$ **then**
8: $C \leftarrow C - p$
9: **end if**
10: **return** $C$

- Let $\mu = -p^{-1} \bmod r = \pm 1$
- Let $\lfloor p/r \rfloor$ have a special form

A. K. Lenstra. Generating RSA moduli with a predetermined portion. Asiacrypt 1998
M. Knežević, F. Vercauteren, and I. Verbauwhede. Speeding up bipartite modular multiplication.WAIFI 2010
T. Acar and D. Shumow. Modular reduction without pre-computation for special moduli. Microsoft Research, 2010
M. Hamburg. Fast and compact elliptic-curve cryptography. Cryptology ePrint Archive, Report 2012/309

# Special primes II - Montgomery friendly primes

**Input:**
$$\begin{cases} A = \sum_{i=0}^{n-1} a_i r^i, B, p, \mu \text{ such that} \\ 0 \le a_i < r,\ 0 \le A, B < r^n, \\ r^{n-1} \le p < r^n, 2 \nmid p, \\ \gcd(r,p) = 1,\ \mu = -p^{-1} \bmod r, \end{cases}$$

**Output:** $\begin{cases} C \equiv A \cdot B \cdot r^{-n} \bmod p \\ \text{such that } 0 \le C < r^n \end{cases}$

1: $C \leftarrow 0$
2: **for** $i = 0$ to $n-1$ **do**
3: $\quad C \leftarrow C + a_i \cdot B$
4: $\quad q \leftarrow \mu \cdot C \bmod r$
5: $\quad C \leftarrow (C + q \cdot p)/r$
6: **end for**
7: **if** $C \ge r^n$ **then**
8: $\quad C \leftarrow C - p$
9: **end if**
10: **return** $C$

- Let $\mu = -p^{-1} \bmod r = \pm 1$
- Let $\lfloor p/r \rfloor$ have a special form
- $2^{127} - 1 = (2^{63} - 1)2^{64} + (2^{64} - 1)$

A. K. Lenstra. Generating RSA moduli with a predetermined portion. Asiacrypt 1998
M. Knežević, F. Vercauteren, and I. Verbauwhede. Speeding up bipartite modular multiplication.WAIFI 2010
T. Acar and D. Shumow. Modular reduction without pre-computation for special moduli. Microsoft Research, 2010
M. Hamburg. Fast and compact elliptic-curve cryptography. Cryptology ePrint Archive, Report 2012/309

# Special primes II - Montgomery friendly primes

**Input:**
$$\begin{cases} A = \sum_{i=0}^{n-1} a_i r^i, B, p, \mu \text{ such that} \\ 0 \le a_i < r,\ 0 \le A, B < r^n, \\ r^{n-1} \le p < r^n, 2 \nmid p, \\ \gcd(r,p) = 1,\ \mu = -p^{-1} \bmod r, \end{cases}$$

**Output:** $\begin{cases} C \equiv A \cdot B \cdot r^{-n} \bmod p \\ \text{such that } 0 \le C < r^n \end{cases}$

1: $C \leftarrow 0$
2: **for** $i = 0$ to $n-1$ **do**
3: $\quad C \leftarrow C + a_i \cdot B$
4: $\quad q \leftarrow \mu \cdot C \bmod r$
5: $\quad C \leftarrow (C + q \cdot p)/r$
6: **end for**
7: **if** $C \ge r^n$ **then**
8: $\quad C \leftarrow C - p$
9: **end if**
10: **return** $C$

- Let $\mu = -p^{-1} \bmod r = \pm 1$
- Let $\lfloor p/r \rfloor$ have a special form
- $2^{127} - 1 = (2^{63} - 1)2^{64} + (2^{64} - 1)$
- $p = 1 + 2^{64} - 2^{66} + 2^{68} - 2^{70} + 2^{72} + 2^{74} + 2^{76} - 2^{79} + 2^{127} = (2^{63} - 27443)2^{64} + 1$
- $\rightarrow$ the modular reduction does not use multiplications


A. K. Lenstra. Generating RSA moduli with a predetermined portion. Asiacrypt 1998
M. Knežević, F. Vercauteren, and I. Verbauwhede. Speeding up bipartite modular multiplication.WAIFI 2010
T. Acar and D. Shumow. Modular reduction without pre-computation for special moduli. Microsoft Research, 2010
M. Hamburg. Fast and compact elliptic-curve cryptography. Cryptology ePrint Archive, Report 2012/309

# And now what?

- We can find cryptographically secure genus-2 curves

**Generic and {2,4}-GLV**

Kohels comprehensive Echidna database
Databases for Elliptic Curves and Higher Dimensional Analogues
`http://echidna.maths.usyd.edu.au/~kohel/dbs`

**Twist-Secure Kummer over $2^{127} - 1$**

P. Gaudry and É. Schost. Genus 2 point counting over prime fields. J. Symb. Comput. 2012

- We have different options for fast reduction
- Let's compare to genus-1 implementations!

# Results

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |

# Results

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |
| surf127eps | 2 | $2^{127} - 735$ | 251 | 236 |

# Results

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |
| surf127eps | 2 | $2^{127} - 735$ | 251 | 236 |
| (a) generic127 | 2 | $2^{127} - 1$ | 254 | 295 |
| (b) generic127 | 2 | $2^{127} - 1$ | 254 | 248 |
| (b) generic128 | 2 | $2^{128} - 173$ | 257 | 364 |

# Results

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |
| surf127eps | 2 | $2^{127} - 735$ | 251 | 236 |
| (a) generic127 | 2 | $2^{127} - 1$ | 254 | 295 |
| (b) generic127 | 2 | $2^{127} - 1$ | 254 | 248 |
| (b) generic128 | 2 | $2^{128} - 173$ | 257 | 364 |
| (a) GLV-4-BK | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 254 | 156 |
| (a) GLV-4-FKT | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 253 | 156 |
| (a) GLV-2-FKT | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 253 | 220 |
| (b) GLV-4-BK | 2 | $2^{128} - 24935$ | 256 | 164 |
| (b) GLV-4-FKT | 2 | $2^{128} - 24935$ | 255 | 167 |
| (b) GLV-2-FKT | 2 | $2^{128} - 24935$ | 255 | 261 |

# Results

| Primitive | $g$ | field char $p$ | $\lceil \log_2(r) \rceil$ | $10^3$ cycles |
|---|---|---|---|---|
| curve25519 | 1 | $2^{255} - 19$ | 253 | 182 |
| Longa-Sica 2-GLV | 1 | $2^{256} - 11733$ | 256 | 145 |
| NISTp-256 | 1 | $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ | 256 | 658 |
| surf127eps | 2 | $2^{127} - 735$ | 251 | 236 |
| (a) generic127 | 2 | $2^{127} - 1$ | 254 | 295 |
| (b) generic127 | 2 | $2^{127} - 1$ | 254 | 248 |
| (b) generic128 | 2 | $2^{128} - 173$ | 257 | 364 |
| (a) Kummer | 2 | $2^{127} - 1$ | 251 | 139 |
| (b) Kummer | 2 | $2^{127} - 1$ | 251 | 117 |
| (b) Kummer | 2 | $2^{128} - 237$ | 253 | 166 |
| (a) GLV-4-BK | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 254 | 156 |
| (a) GLV-4-FKT | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 253 | 156 |
| (a) GLV-2-FKT | 2 | $2^{64} \cdot (2^{63} - 27443) + 1$ | 253 | 220 |
| (b) GLV-4-BK | 2 | $2^{128} - 24935$ | 256 | 164 |
| (b) GLV-4-FKT | 2 | $2^{128} - 24935$ | 255 | 167 |
| (b) GLV-2-FKT | 2 | $2^{128} - 24935$ | 255 | 261 |

# Conclusions

- First implementation of GLV decomposition of genus-2 curves
- Fastest implementation of curve arithmetic at 128-bit security (side channel resistant for free)
- Improved formulas for “generic” hyperelliptic curves

## New family of curves: Kummer chameleons

- In DH protocols: can compute on the Kummer surface
- More complicated schemes: use GLV decomposition
- One curve for multiple purposes!

Open question: GLV decomposition on the Kummer surface?

# Conclusions

- First implementation of GLV decomposition of genus-2 curves
- Fastest implementation of curve arithmetic at 128-bit security (side channel resistant for free)
- Improved formulas for “generic” hyperelliptic curves

## New family of curves: Kummer chameleons

- In DH protocols: can compute on the Kummer surface
- More complicated schemes: use GLV decomposition
- One curve for multiple purposes!

Open question: GLV decomposition on the Kummer surface?
After Asiacrypt 2012, work-in-progress with Ben Smith;
but all suggestions are more than welcome!