A tribute to Pierrick - Parts I & II, followed by A special tribute to Culture Club

Craig Costello

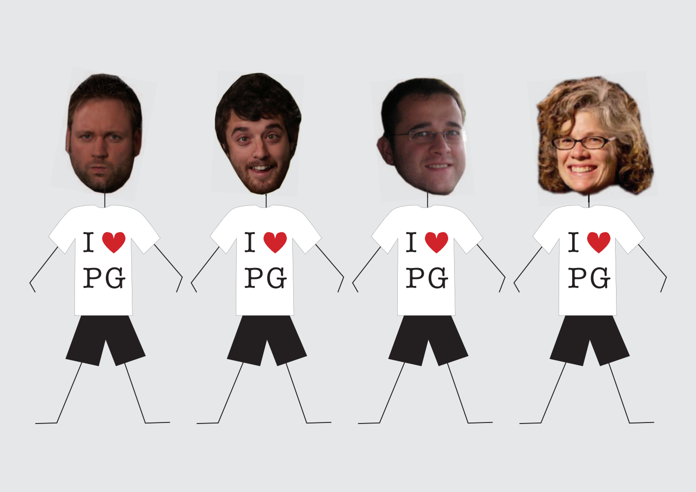
Technische Universiteit Eindhoven

October 29, 2012

ECC2012 - Querétaro, Mexico

A tribute to Pierrick - Part I

Joint work with . . .



Joppe Bos   Craig Costello   Huseyin Hisil   Kristin Lauter

The Kummer surface $\mathcal{K}$: so much faster than $\mathrm{Jac}(C)$

- **2005:** Gaudry proposes working on $\mathcal{K}$ instead of $\mathrm{Jac}(C)$
- $\mathcal{K}$ is (later re-) defined as

$$\mathcal{K}: \quad E'xyzt = ((x^2+y^2+z^2+t^2) - F(xt+yz) - G(xz+yt) - H(xy+zt))^2$$

- $(x,y,z,t) = (\vartheta_1^2(\mathbf{z}), \vartheta_{\mathbf{2}}^{\mathbf{2}}(\mathbf{z}), \vartheta_{\mathbf{3}}^{\mathbf{2}}(\mathbf{z}), \vartheta_{\mathbf{4}}^{\mathbf{2}}(\mathbf{z}))$

  -the squared *fundamental Theta functions*
- E', F, G, H functions of $(\vartheta_1(0)^2, \vartheta_2^2(0), \vartheta_3^2(0), \vartheta_4^2(0))$

  -the squared *fundamental Theta constants*

Curve: Let $p = 2^{128} - 237$ and take $\mathbb{Q}[x]/(x^4 + 25x^2 + 145)$ as quartic CM field.

Then CM method gives Jacobian with $\#\mathrm{Jac} = 16 \cdot r$, r a 253-bit prime, from which an associated $\mathcal{K}$ is given by

$E' = 3323711335547037521537439578541132125887$, $F = 132548732776531240551503236526338110642$,

$G = 198219842417172000280660546928795447629$, $H = 293899164222979967538360298717156893328$.

Timings . . .

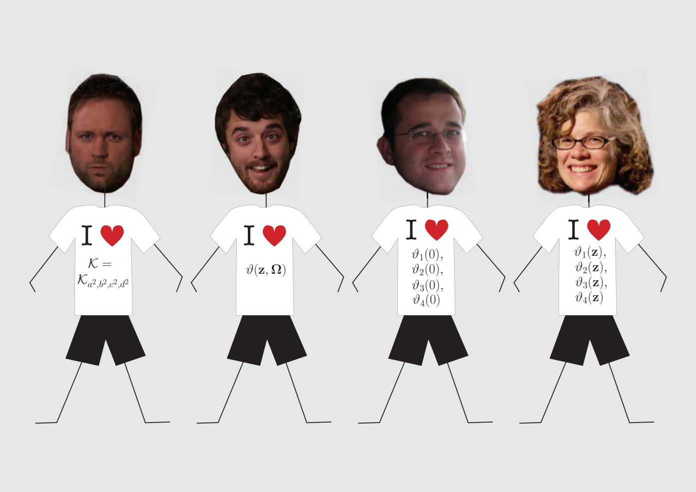
Performance timings (Ivy Bridge) of primitives in 10^3 cycles over prime fields.

Primitive	g	SCR	security	10^3 cycles
Bernstein "curve25519"	1	✓	125.8	182
Hisil "ecfp256e"	1	✗	126.8	227
Longa-Sica "2-GLV"	1	✗	127.0	145
Gaudry-Thome "surf127eps"	2	✓	124.8	236
NISTp-224	1	✓	111.8	302
NISTp-256	1	?	127.8	658
Kummer128	2	✓	125.8	171

- Kummer128: **fastest side-channel resistant implementation over any prime field!**

A tribute to Pierrick - Part 2

Joint work with . . .



A monster computation and a much faster Kummer

- **2010:** Gaudry and Schost find much better twist-secure squares-only Kummer surface, using generic Schoof-Pila (1,000,000 CPU hours)

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

Then $\mathcal{K}$ parameterized by $(a^2, b^2, c^2, d^2) = (11, -22, -19, 3)$ is a Kummer corresponding to a curve C with twist C' whose Jacobians have orders $16 \cdot r$ and $16 \cdot r'$, with r and r' 250- and 251-bit primes respectively.

- Mersenne prime allows much faster arithmetic ...
- some curve constants are small ...

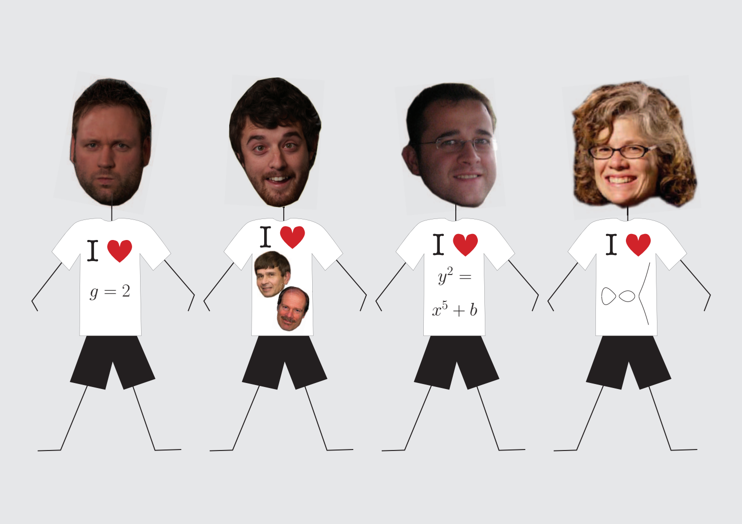
A new speed record.

- **First prime field implementation to break the 140k barrier!**

Primitive	g	SCR	security	10^3 cycles
Bernstein "curve25519"	1	✓	125.8	182
Hisil "ecfp256e"	1	✗	126.8	227
Longa-Sica "2-GLV"	1	✗	127.0	145
Gaudry-Thome "surf127eps"	2	✓	124.8	236
NISTp-224	1	✓	111.8	302
NISTp-256	1	?	127.8	658
Kummer128	2	✓	125.8	171
Kummer127	2	✓	124.8	$\ll 140$

- See http://eprint.iacr.org/2012/XXX.pdf for the speed record!

A tribute to Culture Club



The paper: much more than Kummer

- The Kummer surface implementation is just one aspect of our paper
- Taxonomy of fast algorithms for genus 2 cryptography over prime fields
- Head-to-head comparison of NIST-friendly vs. Montgomery-friendly field arithmetic in all scenarios
- 4-dimensional GLV over Buhler-Koblitz (BK) curves $y^2 = x^5 + b$ and Furukawa-Kawazoe-Takahashi (FKT) curves $y^2 = x^5 + ax$
- Improved formulas for generic hyperelliptic curves
- A tribute to Pierrick - Part III
- And more . . .

Curves offering the best of both worlds

- We use analytic theory to help define a class of curves which offer 4-dimensional GLV decomposition **and** fast arithmetic on the Kummer surface

Let p be any style of prime you like allowing $p \equiv 1 \bmod 20$.

We can amply find twist-secure Buhler-Koblitz curves $C : y^2 = x^5 + b$ with $\mathrm{Jac}(C) = 16 \cdot r$, and which offer both 4-dimensional GLV **and** fast arithmetic on the Kummer surface $\mathcal{K}$.

- Can't say the same if $p \equiv 11 \bmod 20$, or for FKT curves.

- **If you want fastest Diffie-Hellman, use psuedo-addition on $\mathcal{K}$**
- **If you need additions, switch to the BK curve**

Curves offering the best of both worlds . . .

Since these curves allow us to morph to match the scenario, we call them. . .

Kummer Chameleons

Thanks

see http://eprint.iacr.org/2012/XXX.pdf