Hyper-and-elliptic-curve cryptography

(which is not the same as:
hyperelliptic-curve cryptography
and elliptic-curve cryptography)

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Tanja Lange
Technische Universiteit Eindhoven

“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, poorly optimized crypto, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK

“Through our inefficient use of energy (gas guzzling vehicles, badly insulated buildings, **poorly optimized crypto**, etc) we needlessly throw away almost a third of the energy we use.”
—Greenpeace UK (mostly)

DH speed records

Sandy Bridge cycles for high-security constant-time $a, P \mapsto aP$ ("?" if not SUPERCOP-verified):

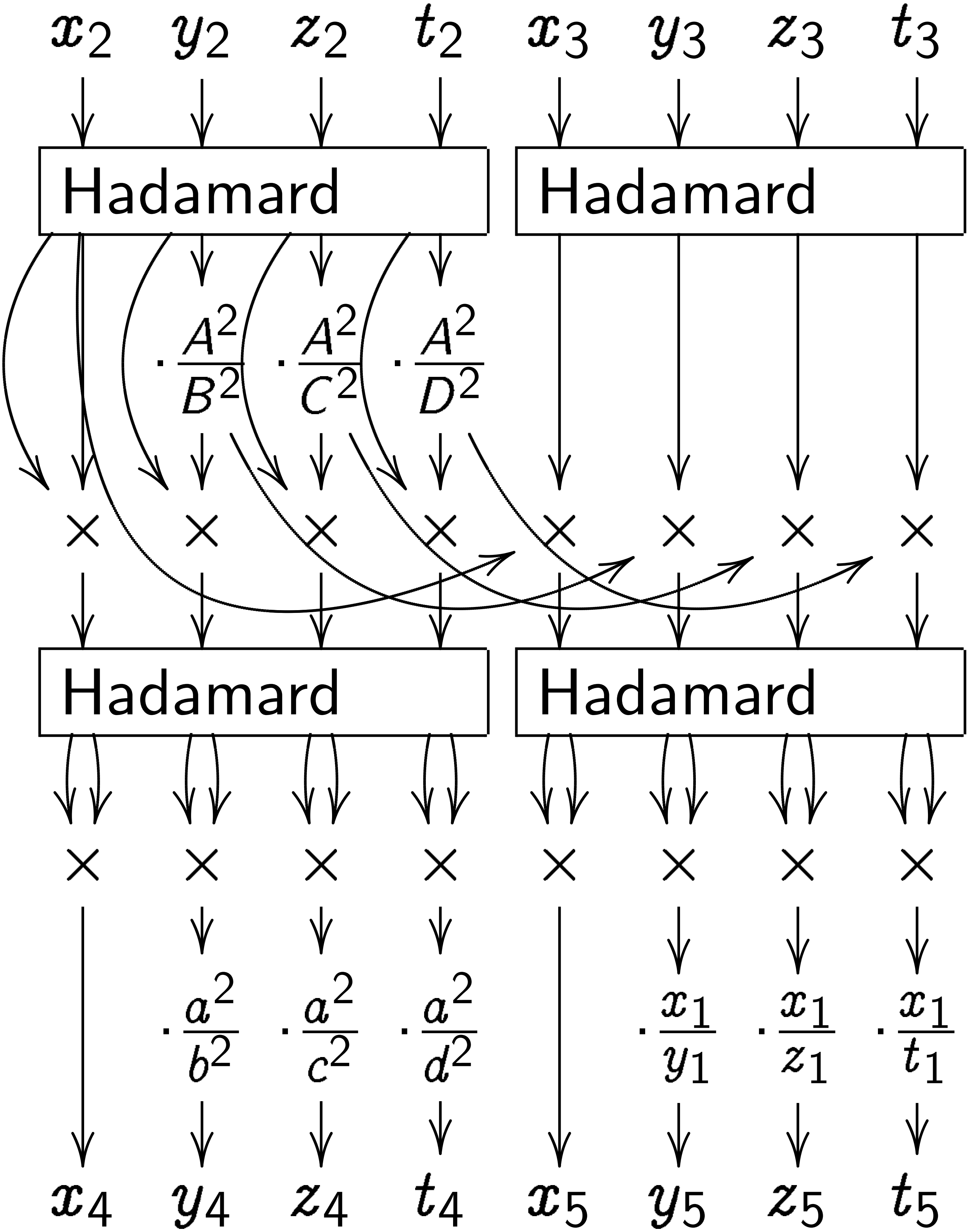
2011 Bernstein–Duif–Lange–Schwabe–Yang:	194036
2012 Hamburg:	153000?
2012 Longa–Sica:	137000?
2013 Bos–Costello–Hisil–Lauter:	122716
2013 Oliveira–López–Aranha–Rodríguez-Henríquez:	114800?
2013 Faz-Hernández–Longa–Sánchez:	96000?
2014 Bernstein–Chuengsatiansup–Lange–Schwabe:	91320

Critical for 122716, 91320:

1986 Chudnovsky–Chudnovsky: traditional Kummer surface allows fast scalar mult. 14**M** for $X(P) \mapsto X(2P)$.

2006 Gaudry: even faster. 25**M** for $X(P), X(Q), X(Q-P) \mapsto X(2P), X(Q+P)$, including 6**M** by surface coefficients.

2012 Gaudry–Schost: 1000000-CPU-hour computation found secure small-coefficient surface over $\mathbf{F}_{2^{127}-1}$.



x_2 y_2 z_2 t_2 x_3 y_3 z_3 t_3
Hadamard
Hadamard
$\cdot\frac{A^2}{B^2}$ $\cdot\frac{A^2}{C^2}$ $\cdot\frac{A^2}{D^2}$
Hadamard
Hadamard
$\cdot\frac{a^2}{b^2}$ $\cdot\frac{a^2}{c^2}$ $\cdot\frac{a^2}{d^2}$
$\cdot\frac{x_1}{y_1}$ $\cdot\frac{x_1}{z_1}$ $\cdot\frac{x_1}{t_1}$
x_4 y_4 z_4 t_4 x_5 y_5 z_5 t_5

Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	new
fast build	**yes**	no	**yes**
any curve	no	**yes**	no
many curves	no	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**
small coeff	no	**yes**	**yes**
fastest DH	no	**yes**	**yes**
fastest keygen	no	no	**yes**
complete add	no	no	**yes**

Strategies to build dim-2 $J/\mathbf{F}_p$ with known $\#J(\mathbf{F}_p)$, large p:

	CM	Pila	Stn	new
fast build	**yes**	no	**yes**	**yes**
any curve	no	**yes**	no	no
many curves	no	**yes**	**yes**	**yes**
secure curves	**yes**	**yes**	**yes**	**yes**
twist-secure	**yes**	**yes**	**yes**	**yes**
Kummer	**yes**	**yes**	**yes**	**yes**
small coeff	no	**yes**	no	**yes**
fastest DH	no	**yes**	no	**yes**
fastest keygen	no	no	no	**yes**
complete add	no	no	no	**yes**

Hyper-and-elliptic-curve crypto

Typical example: Define

$$H : y^2 = (z-1)(z+1)(z+2)$$
$$(z-1/2)(z+3/2)(z-2/3)$$

over $\mathbf{F}_p$ with $p = 2^{127} - 309$;
$J = \operatorname{Jac} H$; traditional Kummer surface K; traditional $X : J \to K$.
Small K coeffs $(20 : 1 : 20 : 40)$.

Hyper-and-elliptic-curve crypto

Typical example: Define
$H: y^2 = (z-1)(z+1)(z+2)$
$\quad (z-1/2)(z+3/2)(z-2/3)$
over $\mathbf{F}_p$ with $p = 2^{127} - 309$;
$J = \operatorname{Jac} H$; traditional Kummer surface K; traditional $X : J \to K$.
Small K coeffs $(20:1:20:40)$.

Warning: There are typos in the Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. We have simpler, computer-verified formulas.

$\#J(\mathbf{F}_p) = 16\ell$
where ℓ is the prime
1809251394333065553493296640760748553649194606010814289531455285792829679923.

Security $\approx 2^{125}$ against rho.

Order of ℓ in $(\mathbf{Z}/p)^*$ is
121529416757478022665490931225631503 87.

Twist security $\approx 2^{75}$.

(Want more twist security?
Switch to $p = 2^{127} - 94825$;
cofactors $16 \cdot 3269239$, 4.)

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

Fast point-counting

Define $\mathbf{F}_{p^2} = \mathbf{F}_p[i]/(i^2+1)$;
$r = (7+4i)^2 = 33+56i$;
$s = 159+56i$; $\omega = \sqrt{-384}$;
$C : y^2 = rx^6 + sx^4 + \overline{s}x^2 + \overline{r}$.

$(x, y) \mapsto (x^2, y)$ takes C to E :
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

$(x, y) \mapsto (1/x^2, y/x^3)$ takes C to
$y^2 = \overline{r}x^3 + \overline{s}x^2 + sx + r$.

$$(z, y) \mapsto \left(\frac{1+iz}{1-iz}, \frac{\omega y}{(1-iz)^3}\right)$$
takes H over $\mathbf{F}_{p^2}$ to C.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

J is isogenous to
Weil restriction W of E, so
computing $\#J(\mathbf{F}_p)$ is fast.

2003 Scholten:
this strategy for
building many genus-2 curves
with fast point-counting.

Handles all elliptic curves
over $\mathbf{F}_{p^2}$ with full 2-torsion
(and more elliptic curves).
Geometrically: all elliptic curves;
codim 1 in hyperelliptic curves.

New: not just point-counting

Alice generates secret $a \in \mathbf{Z}$.
Bob generates secret $b \in \mathbf{Z}$.

Alice computes $aG \in E(\mathbf{F}_{p^2})$
using standard $G \in E(\mathbf{F}_{p^2})$.
Top speed: Edwards coordinates.

Alice sends aG to Bob.

Bob views aG in $W(\mathbf{F}_p)$,
applies isogeny $W(\mathbf{F}_p) \to J(\mathbf{F}_p)$,
computes $b(aG)$ in $J(\mathbf{F}_p)$.
Top speed: Kummer coordinates.

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

In general: use isogenies $\iota : W \to J$ and $\iota' : J \to W$ to dynamically move computations between $E(\mathbf{F}_{p^2})$ and $J(\mathbf{F}_p)$.

But do we have **fast formulas** for ι' and for dual isogeny ι?

Scholten: Define $\phi : H \to E$ as

$$(z, y) \mapsto \left(\frac{(1+iz)^2}{(1-iz)^2}, \frac{\omega y}{(1-iz)^3} \right).$$

Composition of $\phi_2 : (P_1, P_2) \mapsto \phi(P_1)+\phi(P_2)$ and standard $E \to W$ is composition of standard $H \times H \to J$ and some $\iota' : J \to W$.

The conventional continuation:

1. Prove that ι' is an isogeny by analyzing fibers of ϕ_2.

2. Observe that $\iota \circ \iota' = 2$ for some isogeny ι.

3. Compute formulas for ι': take $P_i = (z_i, y_i)$ on $H : y^2 = f(z)$ over $\mathbf{F}_p(z_1, z_2)[y_1, y_2] / (y_1^2 - f(z_1), y_2^2 - f(z_2))$; compose definition of ϕ with addition formulas on E; eliminate z_1, z_2, y_1, y_2 in favor of Mumford coordinates.

4. Simplify formulas for ι'
using, e.g., 2006 Monagan–Pearce
"rational simplification" method.

5. Find ι: norm–conorm etc.

4. Simplify formulas for ι' using, e.g., 2006 Monagan–Pearce "rational simplification" method.

5. Find ι: norm–conorm etc.

Much easier: We applied ϕ_2 to random points in $H(\mathbf{F}_p) \times H(\mathbf{F}_p)$, interpolated coefficients of ι'. Similarly interpolated formulas for ι; verified composition.

Easy computer calculation. "Wasting brain power is bad for the environment."

New: small coefficients

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
. . . unless everything lifts to $\mathbf{Q}$.

New: small coefficients

K defined by 3 coeffs.
Only 2 degrees of freedom in E.

Can't expect small-height coeffs.
... unless everything lifts to $\mathbf{Q}$.

Choose non-square $\Delta \in \mathbf{Q}$;
distinct squares ρ_1, ρ_2, ρ_3
of norm-1 elements of $\mathbf{Q}(\sqrt{\Delta})$;
$r \in \mathbf{Q}(\sqrt{\Delta})$ with $-\rho_1\rho_2\rho_3 = \overline{r}/r$.

Define $s = -r(\rho_1 + \rho_2 + \rho_3)$.
Then $rx^3 + sx^2 + \overline{s}x + \overline{r} =$
$r(x - \rho_1)(x - \rho_2)(x - \rho_3)$.

Choose $\beta \in \mathbf{Q}(\sqrt{\Delta})$ with $\beta \notin \mathbf{Q}$ and $(\overline{\beta}/\beta)^2 \notin \{\rho_1, \rho_2, \rho_3\}$.

Then the Scholten curve $(r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6)y^2 = r(1-\overline{\beta}z)^6 + s(1-\overline{\beta}z)^4(1-\beta z)^2 + \overline{s}(1-\overline{\beta}z)^2(1-\beta z)^4 + \overline{r}(1-\beta z)^6$ has full 2-torsion over $\mathbf{Q}$.

In many cases corresponding Rosenhain parameters λ, μ, ν have $\dfrac{\lambda\mu}{\nu}$ and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}$ both squares in $\mathbf{Q}$, so K is defined over $\mathbf{Q}$. (Degenerate cases: see paper.)

Example: Choose $\Delta = -1$;
$\rho_1 = (i)^2$, $\rho_2 = ((3+4i)/5)^2$,
$\rho_3 = ((5+12i)/13)^2$; $r = 33+56i$,
$s = 159 + 56i$, $\beta = i$.

One Rosenhain choice is
$\lambda = 10$, $\mu = 5/8$, $\nu = 25$.

Then $\dfrac{\lambda\mu}{\nu} = \dfrac{1}{2^2}$

and $\dfrac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)} = \dfrac{1}{40^2}$.

Larger example:
$r = 8648575 - 15615600i$,
$s = -40209279 - 33245520i$;
coeffs $(6137 : 833 : 2275 : 2275)$.