Hyper-and-elliptic-curve cryptography

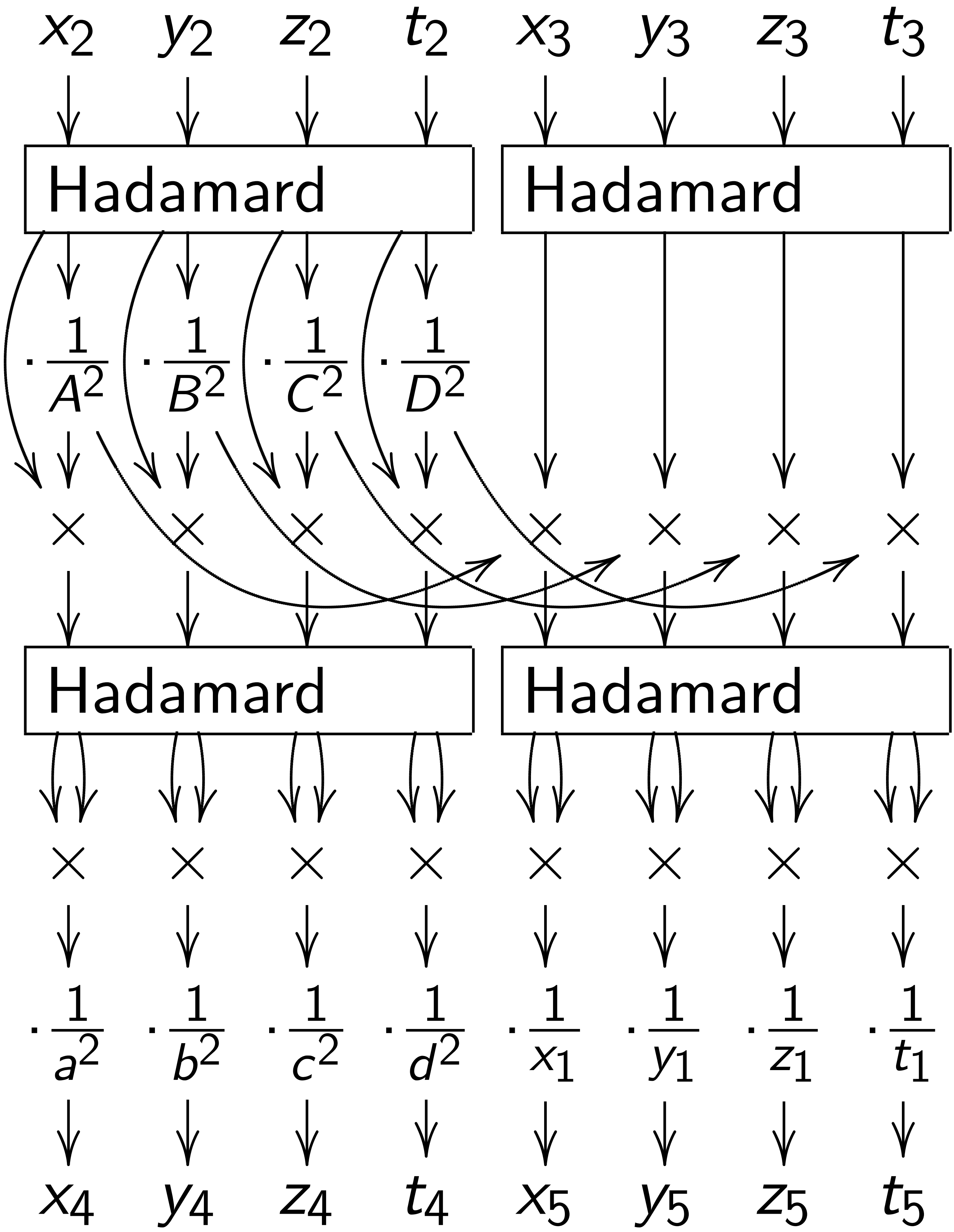
Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Joint work with: Tanja Lange
Technische Universiteit Eindhoven

cr.yp.to/papers.html#hyperand
(2014) + new examples (2015)

Rewind to 2012 Gaudry–Schost:
"the computation took
more than 1,000,000 CPU hours".

The Gaudry–Schost motivation:



Inputs: "squared θ coordinates"

$(x_2 : y_2 : z_2 : t_2)$ for Q_2,

$(x_3 : y_3 : z_3 : t_3)$ for Q_3,

$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes

$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,

$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Inputs: "squared θ coordinates"
$(x_2 : y_2 : z_2 : t_2)$ for Q_2,
$(x_3 : y_3 : z_3 : t_3)$ for Q_3,
$(x_1 : y_1 : z_1 : t_1)$ for $Q_1 = Q_3 - Q_2$.

This diagram computes
$(x_4 : y_4 : z_4 : t_4)$ for $Q_4 = 2Q_2$,
$(x_5 : y_5 : z_5 : t_5)$ for $Q_5 = Q_3 + Q_2$.

Just 14 mults for Q_4
(1986 Chudnovsky–Chudnovsky).
Huge speedup if constants
$\left(\frac{1}{a^2} : \frac{1}{b^2} : \frac{1}{c^2} : \frac{1}{d^2}\right)$ etc. are small.

Just 25 mults for Q_4, Q_5
(2006 Gaudry) after Q_1 precomp.

$(x_i : y_i : z_i : t_i)$ are points on original Kummer surface K :

$$4E^2xyzt = ((x^2 + y^2 + z^2 + t^2) \\ -F(xt + yz) - G(xz + yt) \\ -H(xy + zt))^2$$

where

$$A^2 = a^2 + b^2 + c^2 + d^2,$$
$$B^2 = a^2 + b^2 - c^2 - d^2,$$
$$C^2 = a^2 - b^2 + c^2 - d^2,$$
$$D^2 = a^2 - b^2 - c^2 + d^2,$$
$$F = (a^4 - b^4 - c^4 + d^4)/(a^2d^2 - b^2c^2),$$
$$G = (a^4 - b^4 + c^4 - d^4)/(a^2c^2 - b^2d^2),$$
$$H = (a^4 + b^4 - c^4 - d^4)/(a^2b^2 - c^2d^2),$$
$$E^2 = F^2 + G^2 + H^2 + FGH - 4.$$

Surface is from 1864 Kummer, *Über die Flächen vierten Grades mit sechzehn singulären Punkten*:

Endlich möge hier noch eine Formveränderung erwähnt werden, welche man mit der Gleichung dieser Flächen vornehmen kann. Wählt man die vier in der Form (4.) enthaltenen singulären Tangentialebenen

$$p = 0,\ q = 0,\ p' = 0,\ q' = 0$$

als die Fundamentalebenen, also p, q, p', q', als die vier homogenen Coordinaten, und bezeichnet demgemäfs die beiden letzteren durch r und s, so erhält man folgende Form der Gleichung:

10., $$\phi^2 = 16\,Kpqrs,$$

wo

$$\phi = p^2 + q^2 + r^2 + s^2 + 2a(qr + ps) + 2b(rp + qs) + 2c(pq + rs)$$
$$K = a^2 + b^2 + c^2 - 2abc - 1.$$

in welcher die sieben Constanten a, b, c, d, e, f, k jener Form auf die richtige Anzahl von drei Constanten a, b, c eingeschränkt ist. Wählt man in dieser Form die Coefficienten der linearen Ausdrücke p, q, r, s real, und die drei Constanten a, b, c eben-

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C.
"Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C.
"Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Q_2, Q_3 are points on Jacobian J of a related genus-2 hyperelliptic curve C. "Standard" $X : J/\{\pm 1\} \hookrightarrow\!\!\!\!\rightarrow K$ defines squared θ coords on J.

Use diagram k times to compute $X(Q_1) \mapsto X(nQ_1), X((n+1)Q_1)$ for any $n \in \{0, 1, \ldots, 2^k - 1\}$.

Beware typos in the "standard" Rosenhain/Mumford/Kummer formulas in 2007 Gaudry, 2010 Cosset, 2013 Bos–Costello–Hisil–Lauter. See our paper for simpler formulas **as Sage scripts**.

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

1966 Mumford, *On the equations defining Abelian varieties. I*: "There are several thousand formulas in this paper which allow one *or more* 'sign-like ambiguities': i.e., alternate and symmetric but non-equivalent reformulations. These occur in definitions and theorems. I have made a superhuman effort to achieve consistency and even to make *correct* statements: but I still cannot guarantee the result."

Sage is better than superhuman!

1975 Weil: “Kummer discovered that family of surfaces . . . entirely without the help of the powerful tool provided by theta-functions; actually, the connection with theta-functions was noticed only in 1877, by Cayley and by Borchardt . . . His example is of particular value at a time when it is again realized by algebraic geometers that the detailed study of well-chosen special varieties remains one major road to progress in their field.”

2012 Gaudry–Schost:

"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field:
$\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast.
$\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

2012 Gaudry–Schost:
"We want to find a curve of genus 2 over a prime field that is suitable for building a public-key cryptosystem."

Obvious choice of field: $\mathbf{F}_p$ where $p = 2^{127} - 1$. Fast. $\#J(\mathbf{F}_p) \approx 2^{254}$; big enough.

1000000 CPU hours found $(a^2, b^2, c^2, d^2) = (-11, 22, 19, 3)$, primes $\#J(\mathbf{F}_p)/16, \#J'(\mathbf{F}_p)/16$. Here J' is Jacobian of nontrivial quadratic twist of curve C.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

Is this faster than a similar-security elliptic curve over $\mathbf{F}_{p^2}$ or a similar-size prime field?

Counting ops suggests: Yes, especially with small a^2 etc.

Implementations (2006 Bernstein, 2013 Bos–Costello–Hisil–Lauter, 2014 Bernstein–Chuengsatiansup–Lange–Schwabe): Yes.

2015 Costello–Longa E with $\sqrt{-10}$ CM, 2-isogeny to $\overline{E}$: faster on some CPUs but not others, not compressed, not twist-secure.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J.
So J isn't competitive for key generation, signing, etc.

Summary: Gaudry–Schost J holds speed records for high-security $n, Q \mapsto nQ$.

But what about $P, Q \mapsto P + Q$? $n \mapsto nP$? $m, n, P, Q \mapsto mP + nQ$?

Fastest known addition formulas are faster for E than for J. So J isn't competitive for key generation, signing, etc.

Hyper-and-elliptic curve cryptography: Build *one* group supporting the fastest formulas from genus 1 *and* genus 2.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Group is $E(\mathbf{F}_{p^2}) = W(\mathbf{F}_p)$.
E is an $\mathbf{F}_{p^2}$-complete Edwards curve; W is Weil restriction.
Note: 2 parameters for W.

Map $W(\mathbf{F}_p) \to K(\mathbf{F}_p)$ using fast isogeny $W \to J = \operatorname{Jac} H$ for some H, and fast $X : J \to K$.
Note: 3 parameters for K.

Surprise: We have examples where a^2, b^2, c^2, d^2 are small!
This allows fastest $n, P \mapsto nP$.

Explanation: Can lift from $\mathbf{F}_{p^2}/\mathbf{F}_p$ to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$.

Another virtue of these groups: genus-1 point-counting is fast. (Use Magma; Sage needs $\mathbf{F}_p$.)

History of using $W \to J$ for genus-2 point-counting via genus-1 point-counting:

2002 Gaudry–Hess–Smart in char 2; odd char is “hard”. 2001 Galbraith: “rather difficult”. 2003 Diem, 2003 Diem–Scholten, 2003 Scholten, 2003 Thériault, 2004 Diem–Scholten, 2009 Satoh, 2011 Freeman–Satoh: various odd-char constructions.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1 - \beta z$, $v = 1 - \overline{\beta} z$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1-\beta z$, $v = 1-\overline{\beta}z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curves

(2003 Scholten + simplifications)

Assume: odd prime p;
$r, s, \beta \in \mathbf{F}_{p^2}$; $\beta \notin \mathbf{F}_p$;
minor additional hypotheses.

Write $\overline{r} = r^p$, $\overline{s} = s^p$, $\overline{\beta} = \beta^p$.
Define $g \in \mathbf{F}_{p^2}[z]$ as

$$\frac{rv^6 + sv^4u^2 + \overline{s}v^2u^4 + \overline{r}u^6}{r\overline{\beta}^6 + s\overline{\beta}^4\beta^2 + \overline{s}\overline{\beta}^2\beta^4 + \overline{r}\beta^6}$$

where $u = 1 - \beta z$, $v = 1 - \overline{\beta} z$.
Note that $g \in \mathbf{F}_p[z]$.

Scholten curve $H : y^2 = g(z)$.

Denominator of g is in $\mathbf{F}_p$.

Choose square root $\omega \in \mathbf{F}_{p^2}$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Denominator of g is in $\mathbf{F}_p$.
Choose square root $\omega \in \mathbf{F}_{p^2}$.

Define E as the elliptic curve
$y^2 = rx^3 + sx^2 + \overline{s}x + \overline{r}$.

Define $\phi : H \to E$ as
$(z, y) \mapsto (v^2/u^2, \omega y/u^3)$.

Choose an $\mathbf{F}_p$-basis for $\mathbf{F}_{p^2}$,
hence a Weil restriction W of E.
ϕ induces $H \to W$, which induces
$\iota' : J \to W$ where $J = \operatorname{Jac} H$.

Concretely: $\iota'(P_1 + P_2) =$
W coords of $\phi(P_1) + \phi(P_2)$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J.

Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$.

All formulas are defined over $\mathbf{F}_p$.

Our paper interpolates to obtain low-degree formulas for ι' on Mumford coordinates for J. Also low-degree formulas for $\iota : W \to J$ with $\iota'(\iota(P)) = 2P$. All formulas are defined over $\mathbf{F}_p$.

(Can show: $\iota(P)$ is trace of sum of ϕ-preimages of P; "norm-conorm" map used in, e.g., 2002 Gaudry–Hess–Smart, 2003 Diem, 2004 Arita–Matsuo–Nagao–Shimura. But this doesn't give a very fast algorithm.)

Scholten with fast Kummer?

Given Scholten curve,
compute corresponding
original Kummer surface K:

Factor g into linear factors.

Scholten with fast Kummer?

Given Scholten curve,
compute corresponding
original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation
move to twisted Rosenhain form
$\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Scholten with fast Kummer?

Given Scholten curve,
compute corresponding
original Kummer surface K:

Factor g into linear factors.

By linear-fractional transformation
move to twisted Rosenhain form
$\delta y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Compute

$$b^2 = \sqrt{\frac{\mu(\mu-1)(\lambda-\nu)}{\nu(\nu-1)(\lambda-\mu)}},$$

$$c^2 = \sqrt{\frac{\lambda\mu}{\nu}},\ a^2 = \frac{b^2c^2\nu}{\mu},\ d^2 = 1.$$

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\bar{r}/r$ with $r \in \mathbf{F}^*_{p^2}$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}^*_{p^2}$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\overline{\beta}/\beta)^2 \notin \left\{s_1^2, s_2^2, s_3^2\right\}$.
Then g has 6 distinct roots $(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1, with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$ with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots $(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$; i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.

Take $s_1, s_2, s_3 \in \mathbf{F}_{p^2}$, norm 1,
with s_1^2, s_2^2, s_3^2 distinct.

$-s_1^2 s_2^2 s_3^2$ has norm 1.
Write it as $\overline{r}/r$ with $r \in \mathbf{F}_{p^2}^*$.

Define $s = -r(s_1 + s_2 + s_3)$.

Take any $\beta \in \mathbf{F}_{p^2} - \mathbf{F}_p$
with $(\overline{\beta}/\beta)^2 \notin \{s_1^2, s_2^2, s_3^2\}$.
Then g has 6 distinct roots
$(1 \pm s_j)/(\overline{\beta} \pm \beta s_j) \in \mathbf{F}_p$.

Hope that $a^2, b^2, c^2, d^2 \in \mathbf{F}_p$;
i.e., $\sqrt{\frac{\lambda\mu}{\nu}}, \sqrt{\cdots} \in \mathbf{F}_p$.
Pray for small height.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

<u>Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$</u>

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements $s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$; $g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

Lifting to $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$

$\mathbf{F}_{p^2} = \mathbf{F}_p(\sqrt{\Delta})$ for many **small** squarefree integers Δ.

Take, say, $\beta = \sqrt{\Delta}$.
Take **small** norm-1 elements $s_1, s_2, s_3 \in \mathbf{Q}(\sqrt{\Delta})$.

As before define $r, s \in \mathbf{Q}(\sqrt{\Delta})$; $g \in \mathbf{Q}(\sqrt{\Delta})[z]$; and $\lambda, \mu, \nu \in \mathbf{Q}$.

λ, μ, ν are small.
Maybe the square roots exist, giving small $a^2, b^2, c^2, d^2 \in \mathbf{Q}$.

Or maybe there's an obstruction.

For each small quadratic field:

We tried all small s_1, s_2, s_3.

For each small quadratic field:
We tried all small s_1, s_2, s_3.

For, e.g., $\Delta = -67$ found that
$s_1 = (-17143 + 96\sqrt{\Delta})/17161$,
$s_2 = (189 + 32\sqrt{\Delta})/323$,
$s_3 = (333 - 40\sqrt{\Delta})/467$
produced Scholten curve

$$y^2 = (x - 16/3)(x + 3/1072)$$
$$(x - 1/16)(x + 16/67)$$
$$(x + 1/20)(x - 20/67)$$

with Kummer surface
$a^2 = 194769$, $b^2 = 126939$,
$c^2 = \ 64009$, $d^2 = 126939$.

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

Found many more examples
for various choices of Δ
$\Rightarrow$ thousands of different
$\#E(\mathbf{F}_{p^2})$ for $p = 2^{127} - 1$.

A good example for crypto:

$$y^2 = (z+3)(z+1/9)$$
$$(z-1/7)(z-7/3)$$
$$(z-8/7)(z-7/24).$$

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 32\ell$ for a prime $\ell \approx 2^{249}$.

$\#E'(\mathbf{F}_{p^2}) = 12 \cdot \text{prime}$.
$a^2 = -46893$, $b^2 = 20020$,
$c^2 = \;\; 20020, d^2 = \;\; 5800.$

Another good example:

$$y^2 = (z-1)(z+1/11)$$
$$(z-1/4)(z+4/11)$$
$$(z+5/7)(z-7/55).$$

Another good example:

$$y^2 = (z-1)(z+1/11)$$
$$(z-1/4)(z+4/11)$$
$$(z+5/7)(z-7/55).$$

Slightly lower security level:

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 720\ell$ for a prime $\ell \approx 2^{244.5}$.
$\#E'(\mathbf{F}_{p^2}) = 260 \cdot \text{prime}.$

Another good example:

$$y^2 = (z-1)(z+1/11)$$
$$(z-1/4)(z+4/11)$$
$$(z+5/7)(z-7/55).$$

Slightly lower security level:

$\#J(\mathbf{F}_p) = \#J'(\mathbf{F}_p) = \#E(\mathbf{F}_{p^2})$
$= 720\ell$ for a prime $\ell \approx 2^{244.5}$.
$\#E'(\mathbf{F}_{p^2}) = 260 \cdot \text{prime}$.

Particularly nice arithmetic:

$(a^2 : b^2 : c^2 : d^2) = (20 : 12 : 12 : 5)$;
$(A^2 : \ldots) = (49 : 15 : 15 : 1)$;
$\left(\frac{1}{a^2} : \cdots\right) = (3 : 5 : 5 : 12)$;
$\left(\frac{1}{A^2} : \cdots\right) = (15 : 49 : 49 : 735)$.