Pairings for Cryptographers

Craig Costello

t-craigc@microsoft.com

talk based on disjoint work (not mine) by:

Steven Galbraith, Kenny Paterson, Nigel Smart

August 15, 2012

Pairing groups

- A pairing is a **bilinear** map

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$$
$$P \times Q \longmapsto e(P, Q)$$

- P and Q must come from **linearly independent groups** $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same (prime) order r

Hashing: map-to-point and cofactor multiplication

- $E : y^2 = x^3 + ax + b$
- Assume r is biggest prime factor of $\#E$, h called *cofactor*

$$\#E(\mathbb{F}_q) = h \cdot r$$

- **map-to-point**: Modifying $H : \{0,1\}^* \to \mathbb{F}_q$...
  increment output (i.e. $u \leftarrow u + 1 \in \mathbb{F}_q$) until

$$u^3 + au + b = v^2$$

  for some $v \in \mathbb{F}_q$. Choose between $\pm v$ somehow.
- **cofactor multiplication:** $[h](u, v)$ is now of order r

Hashing: example

- Consider $E : y^2 = x^3 + 4$ over $\mathbb{F}_{11}$
- $\#E(\mathbb{F}_{11}) = 12$
- We want to use biggest prime subgroup order possible ($r = 3$)
- Three points are killed by 3 in $E(\mathbb{F}_q)$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (1,4), (1,7), (2,1), (2,10), (0,2), (0,9), (6,0), (10,5), (10,6), (3,3), (3,8)\}.$$

- A generator is $P = (2, 10)$
- To get a point of order $r = 3$, take $[4]P = (0, 9)$

A hashing example

Suppose $H : \{0,1\}^* \to \mathbb{F}_q$ gives $H(\texttt{str}) = 7$. Then
$\hat{H} : \{0,1\}^* \to E(\mathbb{F}_q)$ gives $\hat{H}(\texttt{str}) = [4](10,5) = (0,2)$

Hashing: example

- Consider $E : y^2 = x^3 + 4$ over $\mathbb{F}_{11}$
- $\#E(\mathbb{F}_{11}) = 12$
- We want to use biggest prime subgroup order possible ($r = 3$)
- Three points are killed by 3 in $E(\mathbb{F}_q)$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (1,4), (1,7), (2,1), (2,10), (0,2), (0,9), (6,0), (10,5), (10,6), (3,3), (3,8)\}.$$

- A generator is $P = (2, 10)$
- To get a point of order $r = 3$, take $[4]P = (0, 9)$

A hashing example

Suppose $H : \{0,1\}^* \to \mathbb{F}_q$ gives $H(\texttt{str}) = 7$. Then
$\hat{H} : \{0,1\}^* \to E(\mathbb{F}_q)$ gives $\hat{H}(\texttt{str}) = [4](10,5) = (0,2)$

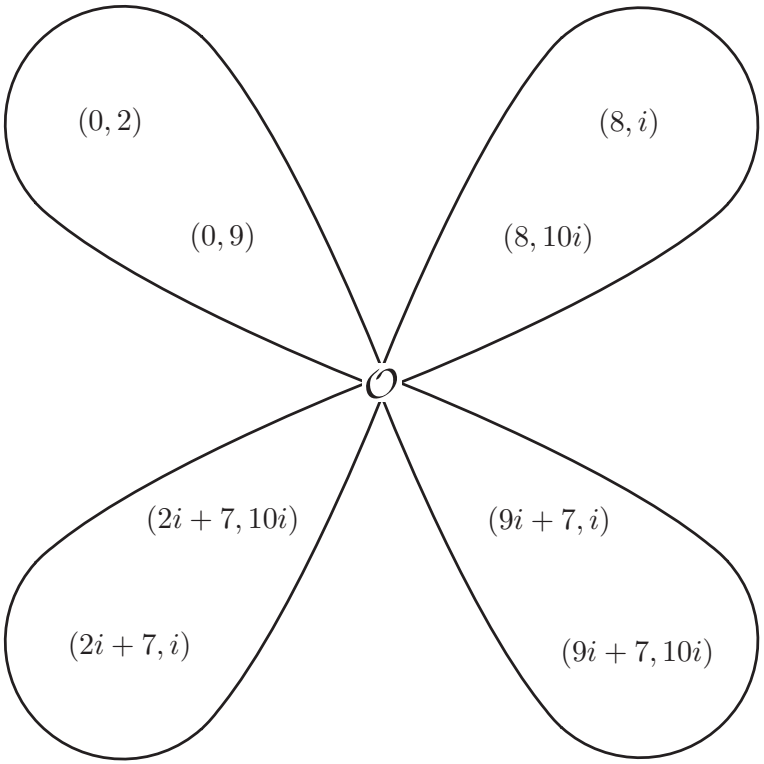
Question: can we now compute a pairing?

- What happens when we extend $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$ with $i^2 = -1$?

$\mathcal{O}$, $(1, 4)$, $(1, 7)$, $(i+6, 10i+7)$, $(i+6, i+4)$, $(i+2, 7i, 1)$, $(i+2, 4i)$, $(8i+1, 3i+3)$, $(8i+1, 8i+8)$, $(4i+3, 5i)$, $(4i+3, 6i)$, $(6i+5, 4i+10)$, $(6i+5, 7i+1)$, $(2, 1)$, $(2, 10)$, $(6i+4, 7i+2)$, $(6i+4, 4i+9)$, $(2i+1, 4i+8)$, $(2i+1, 7i+3)$, $(7i+7, 8i+3)$, $(7i+7, 3i+8)$, $(2i+4, 8)$, $(2i+4, 3)$, $(5i+2, 9i+8)$, $(5i+2, 2i+3)$, $(10i+7, 7i+10)$, $(10i+7, 4i+1)$, $(8i+6, 5)$, $(8i+6, 6)$, $(10i+6, 10i+4)$, $(10i+6, i+7)$, $(5i+4, 4i+2)$, $(5i+4, 7i+9)$, $(4, 8i)$, $(4, 3i)$, $(i+8, 2i+1)$, $(i+8, 9i+10)$, $(3i+3, 9i+3)$, $(3i+3, 2i+8)$, $(4i+8, 0)$, $(5i+1, 9i)$, $(5i+1, 2i)$, $(9i+1, 4i+3)$, $(9i+1, 7i+8)$, $(10i+8, 9i+1)$, $(10i+8, 2i+10)$, **$(8, 10i)$**, **$(8, i)$**, $(8i+5, 4)$, $(8i+5, 7)$, $(9i, 10i+7)$, $(9i, i+4)$, $(10i+2, 7i)$, $(10i+2, 4i)$, $(4i+7, 3i+3)$, $(4i+7, 8i+8)$, $(5, 5i)$, $(5, 6i)$, $(4i+10, 4i+10)$, $(4i+10, 7i+1)$, $(5i+10, 1)$, $(5i+10, 10)$, $(7i+5, 7i+2)$, $(7i+5, 4i+9)$, $(7i, 4i+8)$, $(7i, 7i+3)$, $(3i+1, 8i+3)$, $(3i+1, 3i+8)$, $(9i+4, 8)$, $(9i+4, 3)$, $(8i+3, 9i+8)$, $(8i+3, 2i+3)$, $(7i+10, 7i+10)$, $(7i+10, 4i+1)$, $(10, 5)$, $(10, 6)$, $(10i+5, 10i+4)$, $(10i+5, i+7)$, $(2i+2, 4i+2)$, $(2i+2, 7i+9)$, $(10i+9, 8i)$, $(10i+9, 3i)$, $(3i+10, 2i+1)$, $(3i+10, 9i+10)$, $(6i+2, 9i+3)$, $(6i+2, 2i+8)$, $(7i+8, 0)$, $(9, 9i)$, $(9, 2i)$, $(9i+10, 4i+3)$, $(9i+10, 7i+8)$, $(4i+4, 9i+1)$, $(4i+4, 2i+10)$, **$(9i+7, 10i)$**, **$(9i+7, i)$**, $(3i+5, 4)$, $(3i+5, 7)$, $(i+5, 10i+7)$, $(i+5, i+4)$, $(7, 7i)$, $(7, 4i)$, $(10i+3, 3i+3)$, $(10i+3, 8i+8)$, $(7i+3, 5i, 1)$, $(7i+3, 6i)$, $(i+7, 4i+10)$, $(i+7, 7i+1)$, $(6i+10, 1)$, $(6i+10, 10)$, $(9i+2, 7i+2)$, $(9i+2, 4i+9)$, $(2i+10, 4i+8)$, $(2i+10, 7i+3)$, $(i+3, 8i+3)$, $(i+3, 3i+8)$, $(3, 8)$, $(3, 3)$, $(9i+6, 9i+8)$, $(9i+6, 2i+3)$, $(5i+5, 7i+10)$, $(5i+5, 4i+1)$, $(3i+6, 5)$, $(3i+6, 6)$, $(2i, 10i+4)$, $(2i, i+7)$, $(4i+5, 4i+2)$, $(4i+5, 7i+9)$, $(i+9, 8i)$, $(i+9, 3i)$, $(7i+4, 2i+1)$, $(7i+4, 9i+10)$, $(2i+6, 9i+3)$, $(2i+6, 2i+8)$, $(6, 0)$, $(6i+1, 9i)$, $(6i+1, 2i)$, $(4i, 4i+3)$, $(4i, 7i+8)$, $(8i+10, 9i+1)$, $(8i+10, 2i+10)$, **$(2i+7, 10i)$**, **$(2i+7, i)$**, **$(0, 2)$**, **$(0, 9)$**

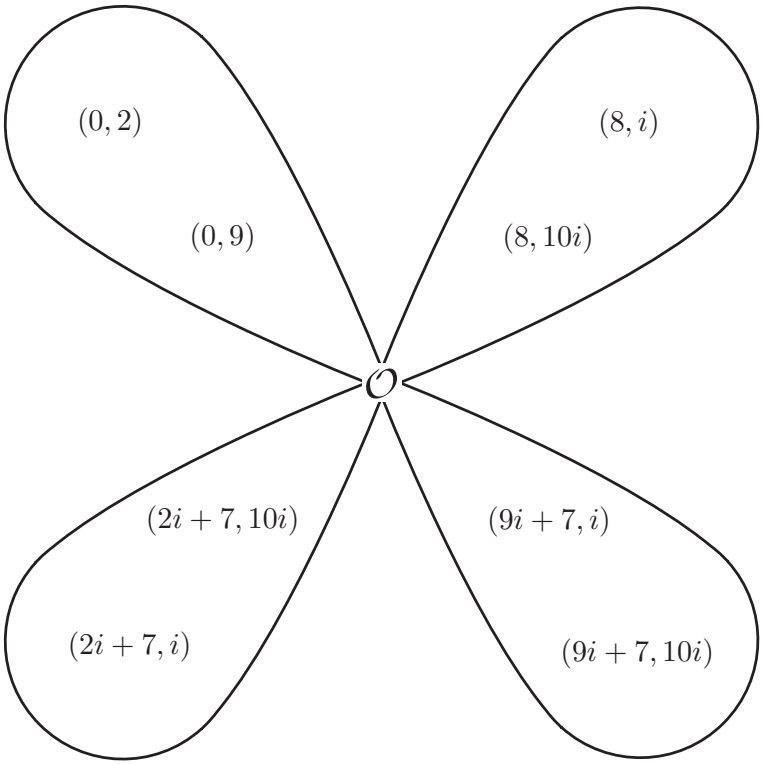
- There's now 9 points that are killed by 3

Torsion points



- 3 points in $E(\mathbb{F}_q)[3]$
- 9 points in $E(\mathbb{F}_{q^2})[3]$ (4 cyclic subgroups of order 3)

Torsion points



- 3 points in $E(\mathbb{F}_q)[3]$
- 9 points in $E(\mathbb{F}_{q^2})[3]$ (4 cyclic subgroups of order 3)
- **Question: How many points in**
  $E(\mathbb{F}_{q^3})[3]$, $E(\mathbb{F}_{q^4})[3]$,...**?**

In general...

- No matter how far we extend $\mathbb{F}_q$, there is precisely r^2 points that are killed by r
- They form $r+1$ cyclic subgroups of order r (they all share $\mathcal{O}$)
- In the previous example, all points killed by 3 were contained in $\mathbb{F}_{q^2}$

Thm: Balasubramanian-Koblitz

Minimal $k \in \mathbb{Z}$ such that $r \mid q^k - 1$
$\rightarrow$ all r^2 points killed by r lie in $E(\mathbb{F}_{q^k})$

- **r points in $E(\mathbb{F}_q)$ killed by r, but once we find one more in $E(\mathbb{F}_{q^k})$, we find them all!**

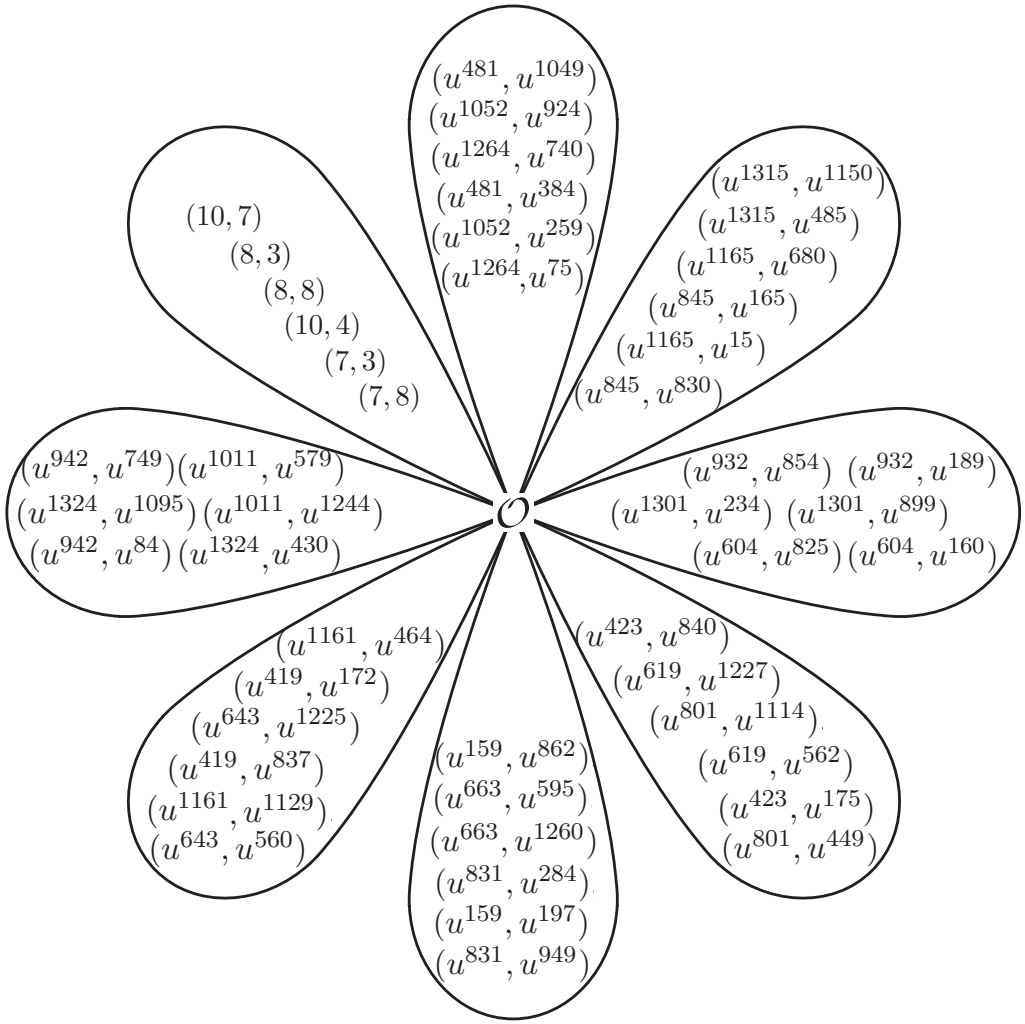
Another example

- Consider $E : y^2 = x^3 + 7x + 2$ over $\mathbb{F}_{11}$
- $\#E(\mathbb{F}_{11}) = r = 7$

$$E(\mathbb{F}_{11}) = \{\mathcal{O}, (7,3), (7,8), (8,3), (8,8), (10,4), (10,7)\}.$$

- $q = 11$, $r = 7$, minimum k such that $q^k - 1$ is $k = 3$
- $\mathbb{F}_{q^3} = \mathbb{F}_q[u]/(u^3 + u + 4)$
- $\#E(\mathbb{F}_{11^3}) = 2^2 \cdot 7^3$
  - 7 points killed by 7 in $E(\mathbb{F}_q)$
  - 7 points killed by 7 in $E(\mathbb{F}_{q^2})$
  - 49 points killed by 7 in $E(\mathbb{F}_{q^3})$
  - 49 points killed by 7 in $E(\mathbb{F}_{q^4})$
  - ...
  - 49 points killed by 7 in $E(\overline{\mathbb{F}}_q)$

Another example: the 7-torsion

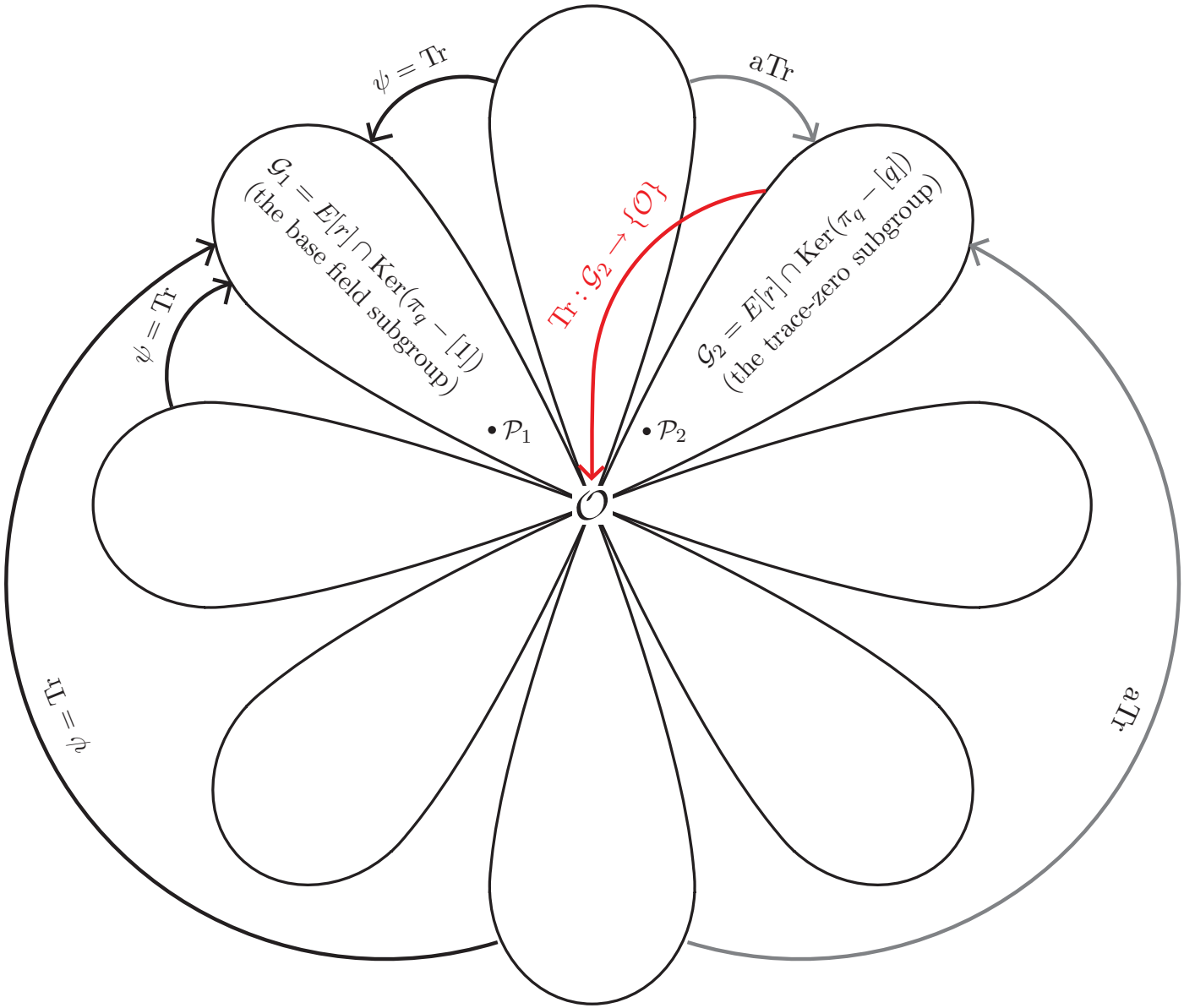


- The 7-torsion of $E : y^2 = x^3 + 7x + 2$ over $\mathbb{F}_{11^3}$

What do cryptographers want in a pairing?

- Of the $(r+1)$ cyclic subgroups of order r in $E(\mathbb{F}_{q^k})$, we need to define two linearly independent subgroups $\mathbb{G}_1$ and $\mathbb{G}_2$
- The main three properties cryptographers might want
  1. to be able to **hash onto** $\mathbb{G}_1$ **and** $\mathbb{G}_2$ (randomly sample)
  2. **an isomorphism** $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ for the security proof to work
  3. the pairing to be as **efficient** as possible
- **Crux of talk: all three not possible simultaneously...**

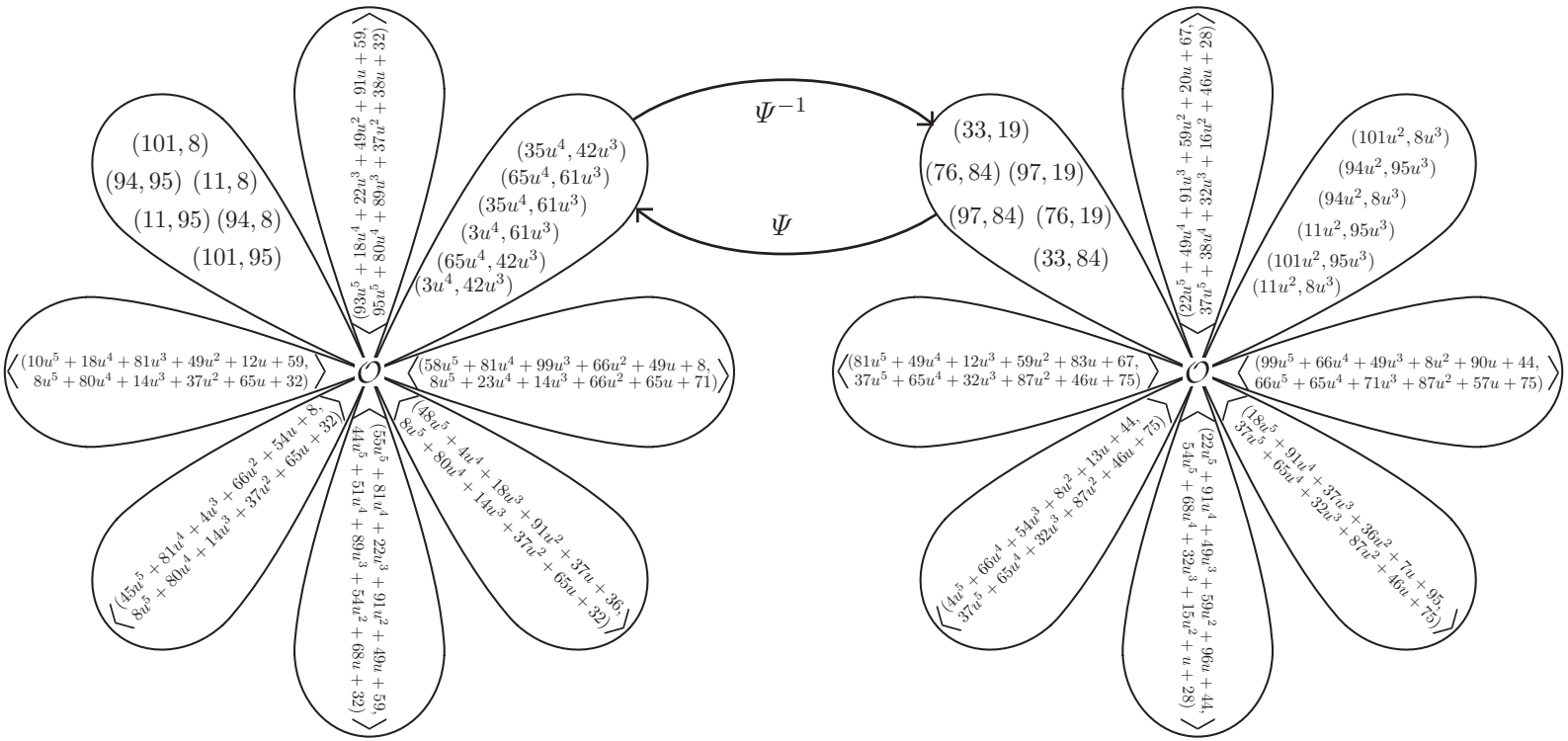
Maps on the general torsion (ordinary curves)



The twisted curve

- **The original curve (left)**

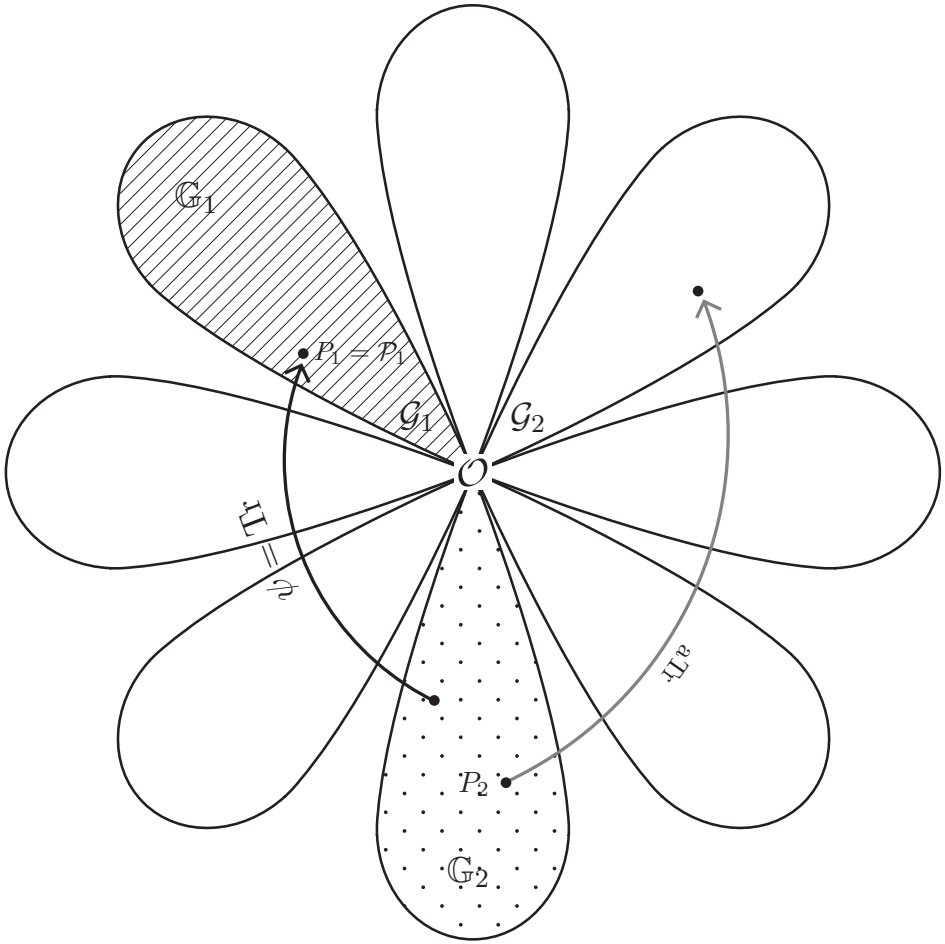
$(q = 103, \quad E/\mathbb{F}_q : y^2 = x^3 + 72, \quad \#E(\mathbb{F}_q) = 84, \quad r = 7, \quad k = 6, \quad \mathbb{F}_{q^k} = \mathbb{F}_q[u]/(u^6 + 2))$



- **The twisted curve (right)**

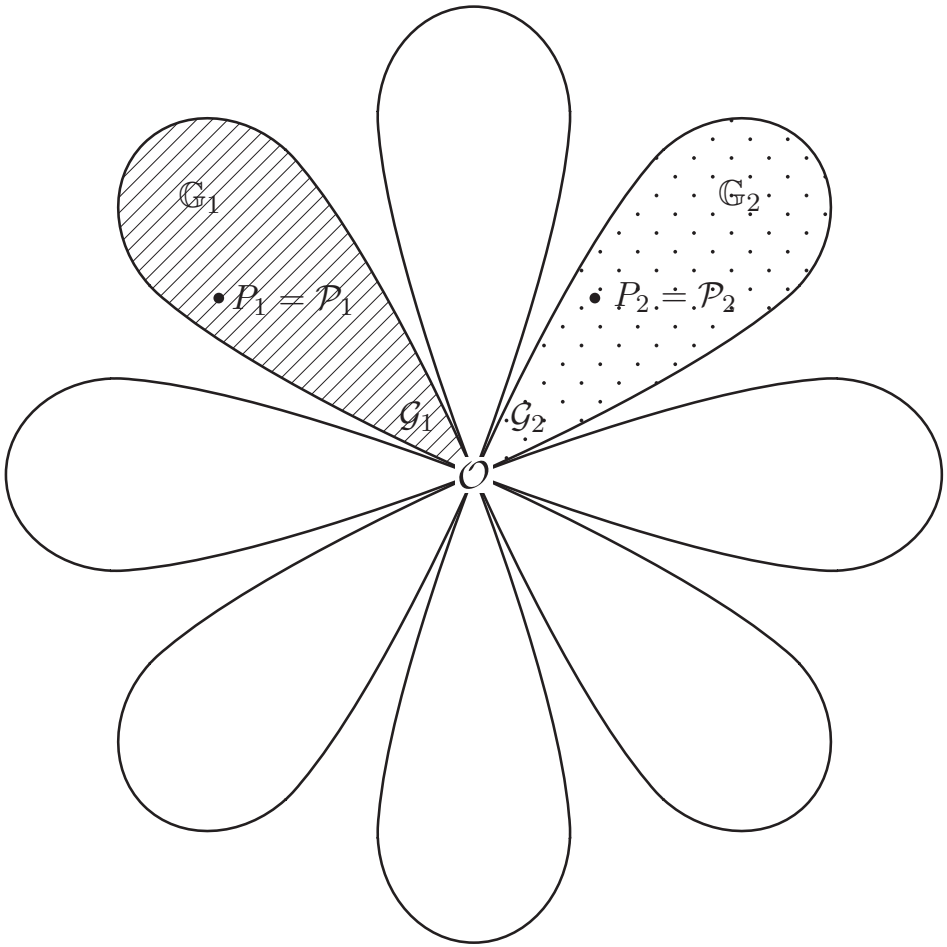
$(q = 103, \quad E/\mathbb{F}_q : y^2 = x^3 - 41, \quad \#E(\mathbb{F}_q) = 91, \quad r = 7, \quad k = 6, \quad \mathbb{F}_{q^k} = \mathbb{F}_q[u]/(u^6 + 2))$

Type 2 pairing



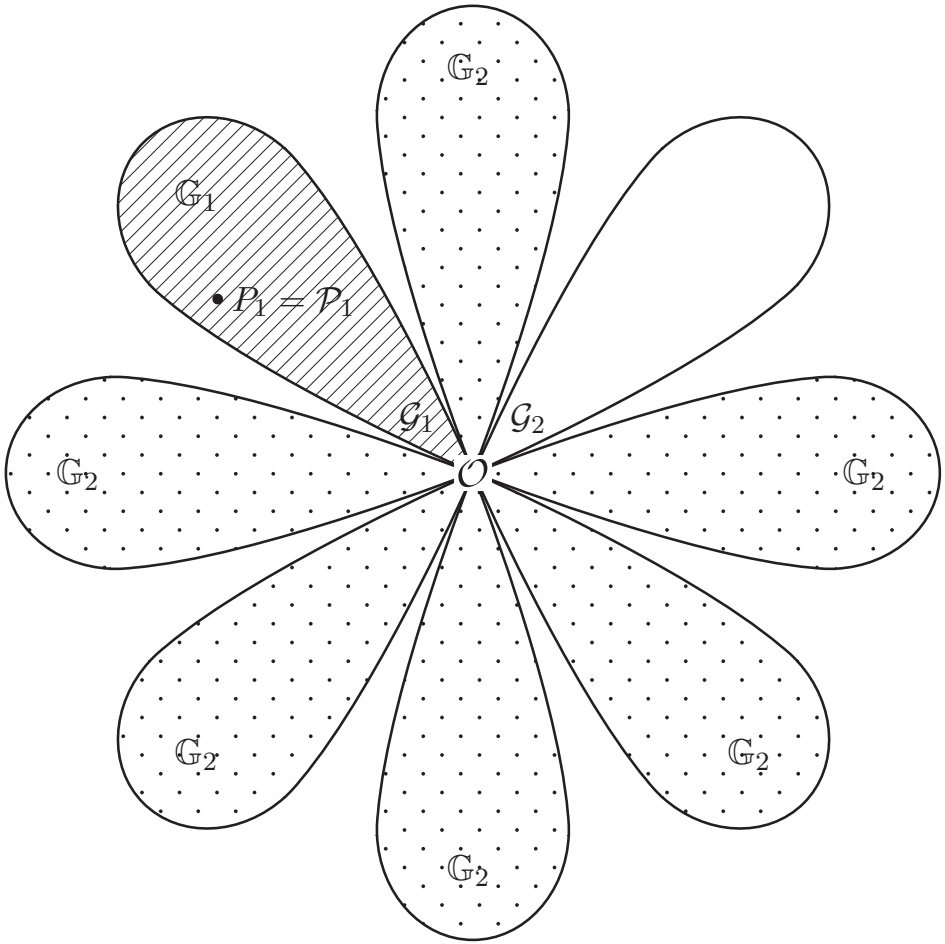
Drawback: can't hash onto $\mathbb{G}_2$ without knowing the ECDLP w.r.t. the generator

Type 3 pairing



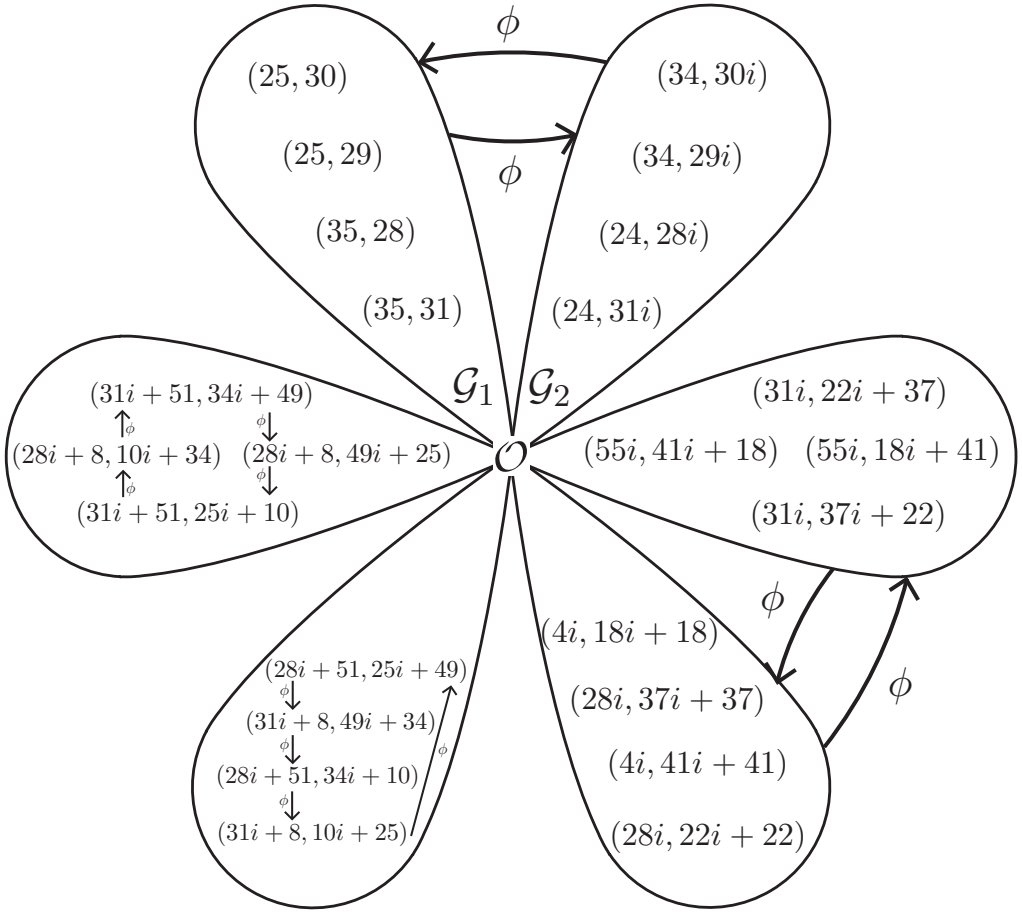
Drawback: can't compute $\psi : \mathbb{G}_2 \to \mathbb{G}_1$

Type 4 pairing (Shacham's thesis)



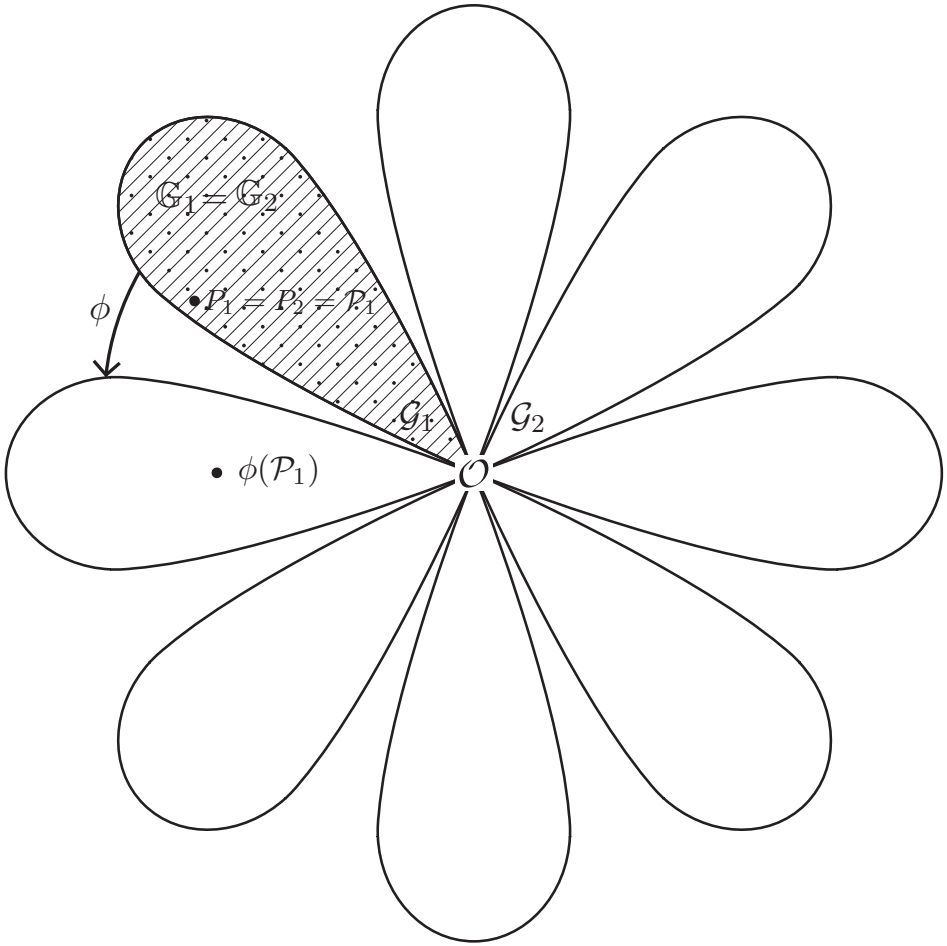
Drawback: elements of $\mathbb{G}_2$ linearly independent

Type 1: Supersingular curves have distortion maps



$E : y^2 = x^3 + x$ over $\mathbb{F}_{59^2} = \mathbb{F}_{59}[i]/(i^2 + 1)$,
map $\phi : (x, y) \mapsto (-x, iy)$: can map out of $\mathbb{G}_1$

Type 1 pairing



Drawback: curve must be supersingular, meaning $k \leq 6$ for elliptic curves - either much less secure or much less efficient

Motivation for "Pairings for ~~Dummies~~ Cryptographers"

- Authors commonly write $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, and/or assume all properties (isomorphism, hashing, symmetry, etc)
- On the one hand, fair enough: pairings as a black-box
- On the other hand, it's a cop out (especially if you have huge products of pairings etc, and want to claim scheme is "efficient" - or dare to claim/cite timings)
- Recommended reading for those that think they need ψ
  1. Chatterjee-Menezes: ".... - The Role of ψ Revisisted" - Type 2 pairings offer no benefit over Type 3 pairings.
  2. also see Smart-Vercauteren: "On computable isomorphisms in efficient pairing-based systems"
- If you don't need ψ, Type 3 pairings are the best

Match your protocol to the best type (modulo caveats)

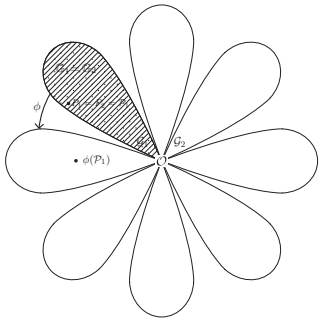


Figure: Type 1 pairings **(if you don't need efficiency/security)**.

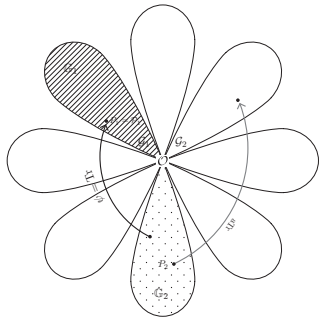


Figure: Type 2 pairings **(if you don't need to randomly sample from $\mathbb{G}_2$)**.

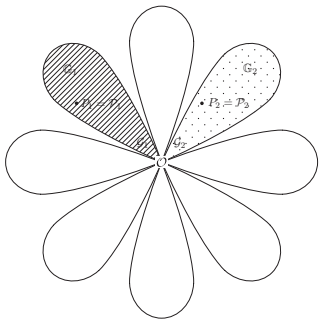


Figure: Type 3 pairings **(if your proof doesn't need/want a computable $\psi : \mathbb{G}_2 \to \mathbb{G}_1$)**. see next slide

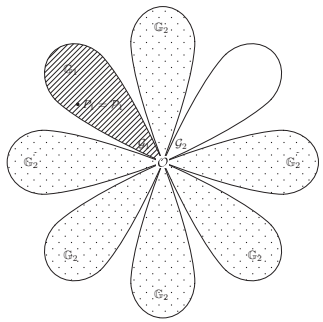


Figure: Type 4 pairings **(if elements of $\mathbb{G}_2$ can be linearly independent)**.

Questions...

In the question time of this talk, it was pointed out to me that I'd missed an important point: namely, that some schemes that are based on the *external Diffie-Hellman assumption* (XDH) or its variants actually rely on the non-existence of an efficiently computable $\psi : \mathbb{G}_2 \to \mathbb{G}_1$, i.e. where Type 3 pairings are a must have. This is because such schemes require the decisional Diffie-Hellman problem to also be hard in $\mathbb{G}_2$, which is not the case if ψ is efficiently computable.