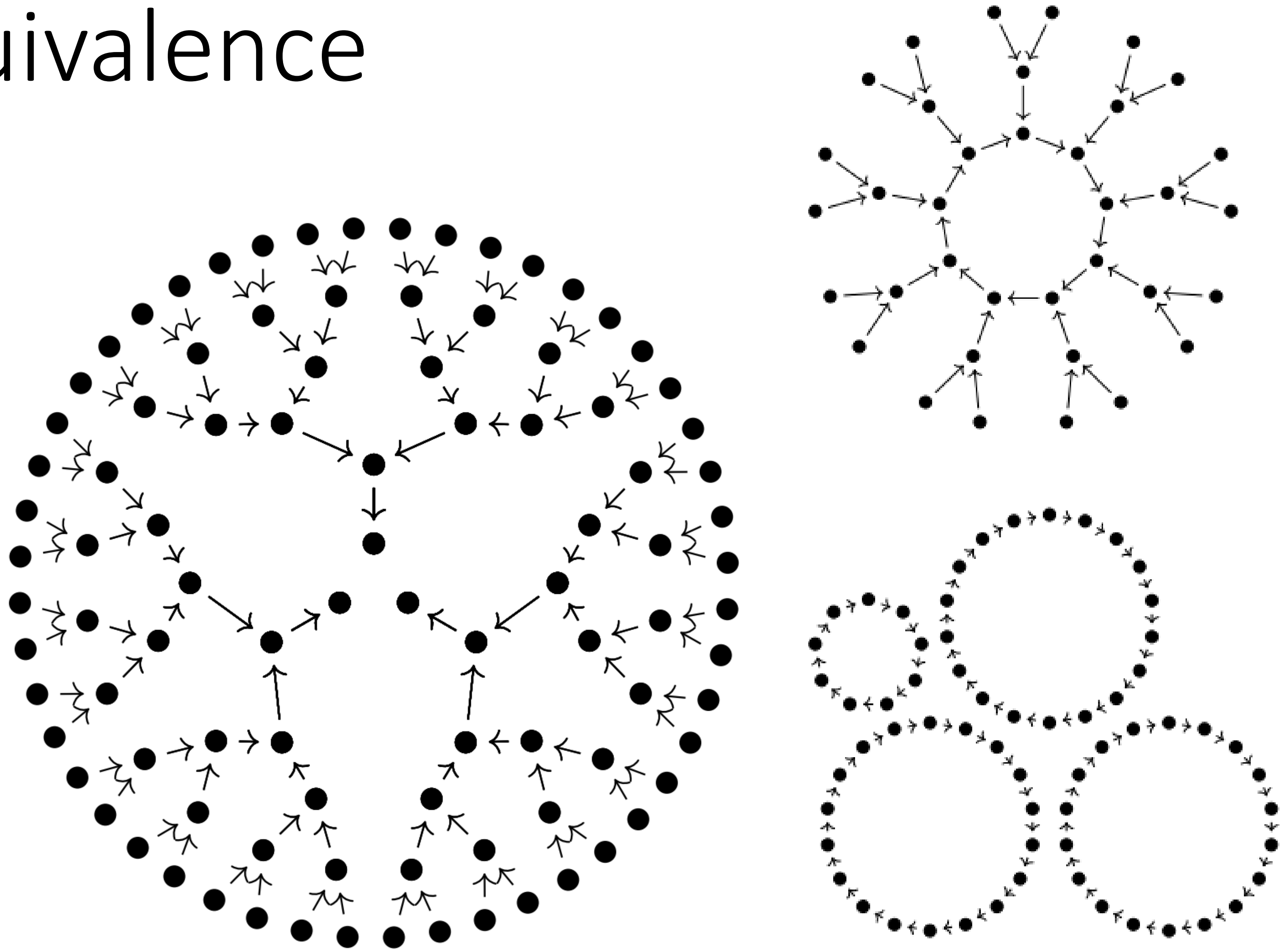
Algorithms for the Alternating Trilinear Form Equivalence Problem

Ward Beullens

IBM **Research** Europe

Crypto ‘23



Alternating Trilinear Form Equivalence

Let V be a vector space of dimension n over a finite field K with q elements.

Definition (alternating trilinear form):
$\phi: V^3 \to K$ is an alternating trilinear form if:
1) ϕ is K-linear in each of its 3 arguments (trilinear)

e.g., $\phi(\alpha u + \beta u', v, w) = \alpha\phi(u, v, w) + \beta\phi(u', v, w)$

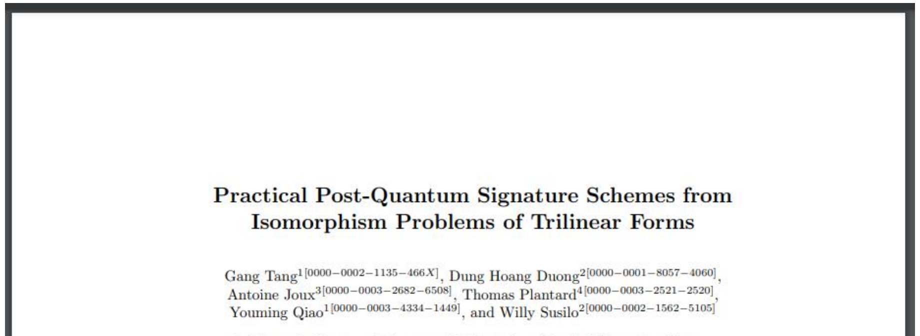
2) $\phi(u, v, w) = 0$ if $u = v, u = w$, or $v = w$ (alternating)

Definition (equivalence): We say two alternating trilinear forms ϕ_1, ϕ_2 are equivalent if there exists $S \in GL(V)$ such that for all $u, v, w \in V$

$$\phi_2(u, v, w) = \phi_1(Su, Sv, Sw)\,.$$

Given equivalent alternating trilinear forms ϕ_1, ϕ_2, how to find an equivalence S?

This problem was recently used to construct cryptography,
in particular, for $n = \dim(V) \in \{9,10,11\}$

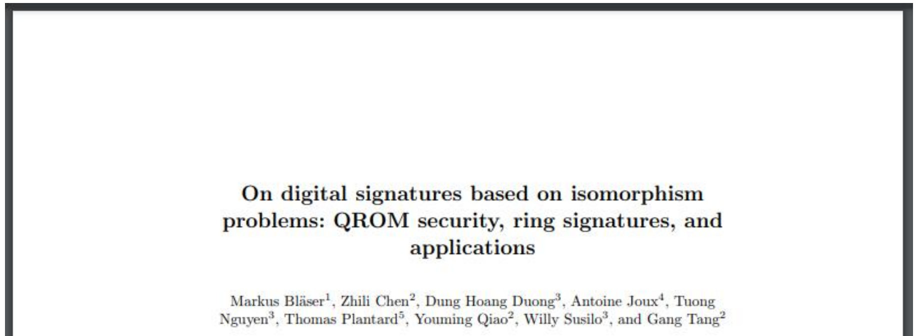


Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms

Gang Tang[1][0000−0002−1135−466X], Dung Hoang Duong[2][0000−0001−8057−4060], Antoine Joux[3][0000−0003−2682−6508], Thomas Plantard[4][0000−0003−2521−2520], Youming Qiao[1][0000−0003−4334−1449], and Willy Susilo[2][0000−0002−1562−5105]

[1] Centre for Quantum Software a
Faculty of Engineering and Informati
NS
Youming.Qiao@uts.edu.a
[2] Institute of Cybersecurity and Cr
Technology, University of Wollongo
{hduong,
[3] CISPA Helmholtz Center for I
j
[4] Emerging Technology R
tplan

Abstract. In this paper, we
on the alternating trilinear f
inspired by the Goldreich-Mi
for graph isomorphism, and
for the NIST's post-quantum
First, we present theoretical e
in the post-quantum cryptog
from several research lines, in
variate cryptography, cryptogr
random oracle model, and rec
algebraic structures in algorit

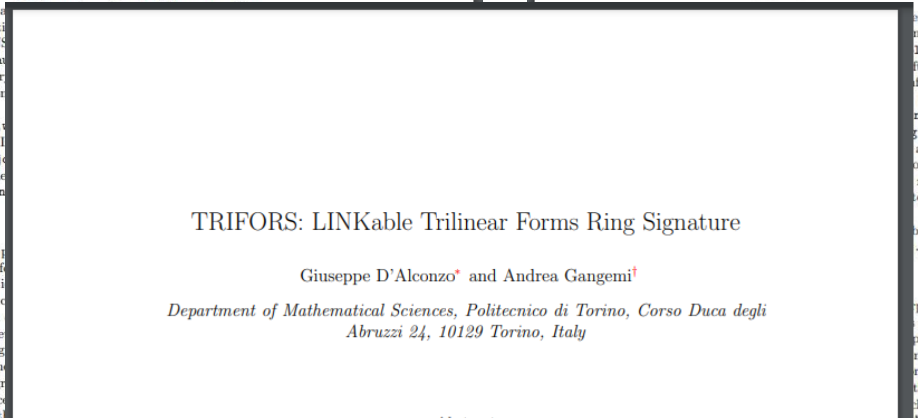


On digital signatures based on isomorphism problems: QROM security, ring signatures, and applications

Markus Bläser[1], Zhili Chen[2], Dung Hoang Duong[3], Antoine Joux[4], Tuong Nguyen[3], Thomas Plantard[5], Youming Qiao[2], Willy Susilo[3], and Gang Tang[2]

r Science, Saarland University, Saarland
mpus, Saarbrücken, Germany.
laeser@cs.uni-saarland.de
ftware and Information, School of Comp
formation Technology, University of Tec
Ultimo, NSW, Australia.
nt.uts.edu.au, Youming.Qiao@uts.edu
.tang-1@student.uts.edu.au
and Cryptology, School of Computing a
of Wollongong, Wollongong, NSW 2522,
ntn807@uowmail.edu.au, wsusilo@uow
er for Information Security, Saarbrücke
joux@cispa.de
s, Murray Hill, New Jersey, United Stat
.plantard@nokia-bell-labs.com

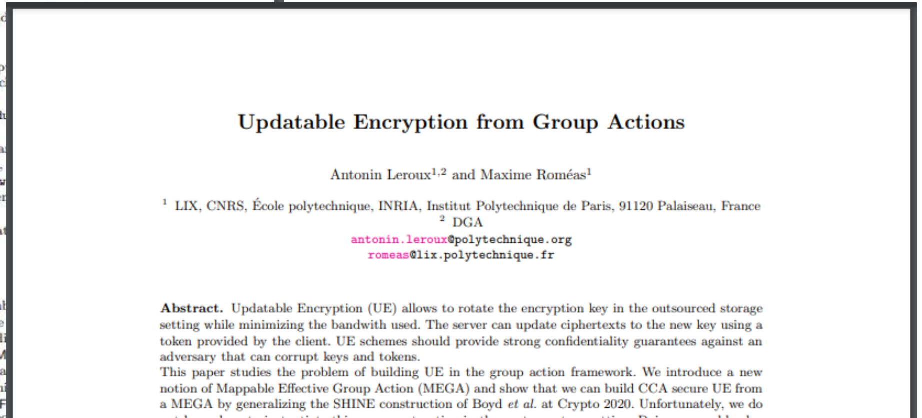
phism problem asks whether two comb
are essentially the same. Based on the
phism problem, there is a well-known di
n the Goldreich–Micali–Widgerson (GM
r graph isomorphism and the Fiat–Sha
tly, there is a revival of activities on th
hemes SeaSign (Eurocrypt 2019), CSI-F



TRIFORS: LINKable Trilinear Forms Ring Signature

Giuseppe D'Alconzo* and Andrea Gangemi†

Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy



Updatable Encryption from Group Actions

Antonin Leroux[1,2] and Maxime Roméas[1]

[1] LIX, CNRS, École polytechnique, INRIA, Institut Polytechnique de Paris, 91120 Palaiseau, France
[2] DGA
antonin.leroux@polytechnique.org
romeas@lix.polytechnique.fr

Abstract. Updatable Encryption (UE) allows to rotate the encryption key in the outsourced storage setting while minimizing the bandwith used. The server can update ciphertexts to the new key using a token provided by the client. UE schemes should provide strong confidentiality guarantees against an adversary that can corrupt keys and tokens.
This paper studies the problem of building UE in the group action framework. We introduce a new notion of Mappable Effective Group Action (MEGA) and show that we can build CCA secure UE from a MEGA by generalizing the SHINE construction of Boyd *et al.* at Crypto 2020. Unfortunately, we do

Summary of results:

New algorithms for the ATFE problem for small n

$dim(V)$	Tang et al.	This work
9	$\tilde{O}(q^7)$	$\tilde{O}(q)$
10	$\tilde{O}(q^7)$	$\tilde{O}(q^6)$
11	$\tilde{O}(q^9)$	$\tilde{O}(q^4)$

This talk

For $n = 10$ we have an algorithm that runs in $O(1)$ field operations but that only works with probability $\sim 1/q$ over the choice of (ϕ_1, ϕ_2)
($\sim$1 hour of laptop time and probability 2^{-17} for proposed parameters)

We use a black box [Bouillaguet et al., 2011]

$\phi_1, \phi_2 = \phi_1 \circ S$
$u, v = Su$
$u \neq 0$

S

Guessing Su gives an algorithm with complexity $O\big(q^n \cdot poly(n)\big)$.

Invariants

We say an invariant is a function

$$F(\phi, u): ATF(V) \times V \to X$$

such that

$$\forall S \in GL(V) \quad F(\phi, u) = F\left(\phi \circ S, S^{-1}u\right)$$

The dream is to find a “perfect” invariant i.e.

$F(\phi_1, u) = F(\phi_2, v) \iff \exists S: \phi_2 = \phi_1 \circ S$ and $v = S^{-1}u$

We then only need to find u, v such that $F(\phi_1, u) = F(\phi_2, v)$,
and use 

Attempt 0: rank

Given ϕ, u it is natural to look at the bilinear form

$$\phi_u(.,.) \coloneqq \phi(u,.,.)$$

Any invariant of ϕ_u is an invariant of (ϕ, u). E.g., the rank.

$$F(\phi, u) \coloneqq rank(\phi_u)$$

Attempt 1: Graph-based invariants

We can define a graph G_4 whose vertices are the projective points of rank 4.

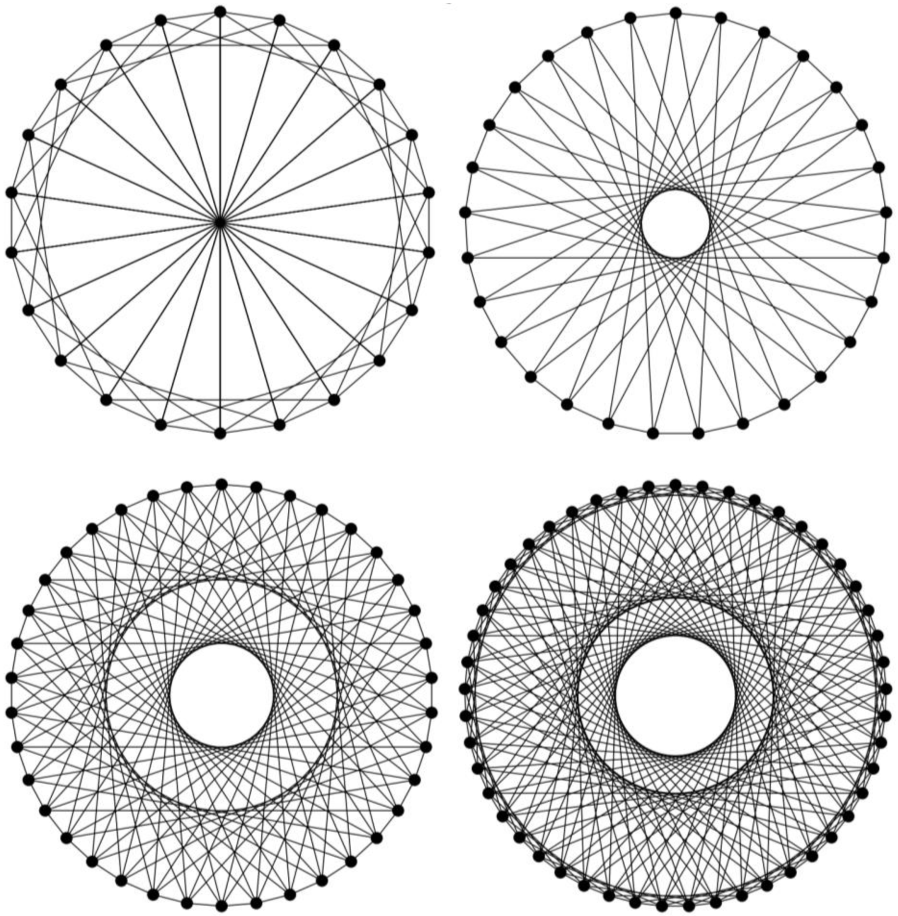
$$\{\boldsymbol{u} \in P(V) \mid \phi_u \; has \; rank \; 4\}$$

and where two vertices u, v share an edge if

$$\phi(\boldsymbol{u}, \boldsymbol{v}, .) = 0$$

Lemma: For random ϕ in dimension 9 this graph has on average $q^2 + O(q)$ vertices, and $q^3/2 + O(q^2)$ edges.

An isomorphism of forms induces an isomorphism of the graphs, so we can use the neighborhood of u as an invariant.



Very often these graphs are regular and have dihedral symmetry!

Rank-4 points form a Torsor

[Benedetti, Manivel, and Tanturri. 2019]

Chord-tangent group law on points of elliptic curve:

Given 2 generic points P, Q, there is a 3rd point on the line PQ, say $P * Q$

Pick identity O, then group law is

$$P + Q \coloneqq O * (P * Q)$$

"Chord-tangent" group law on rank-4 projective points:

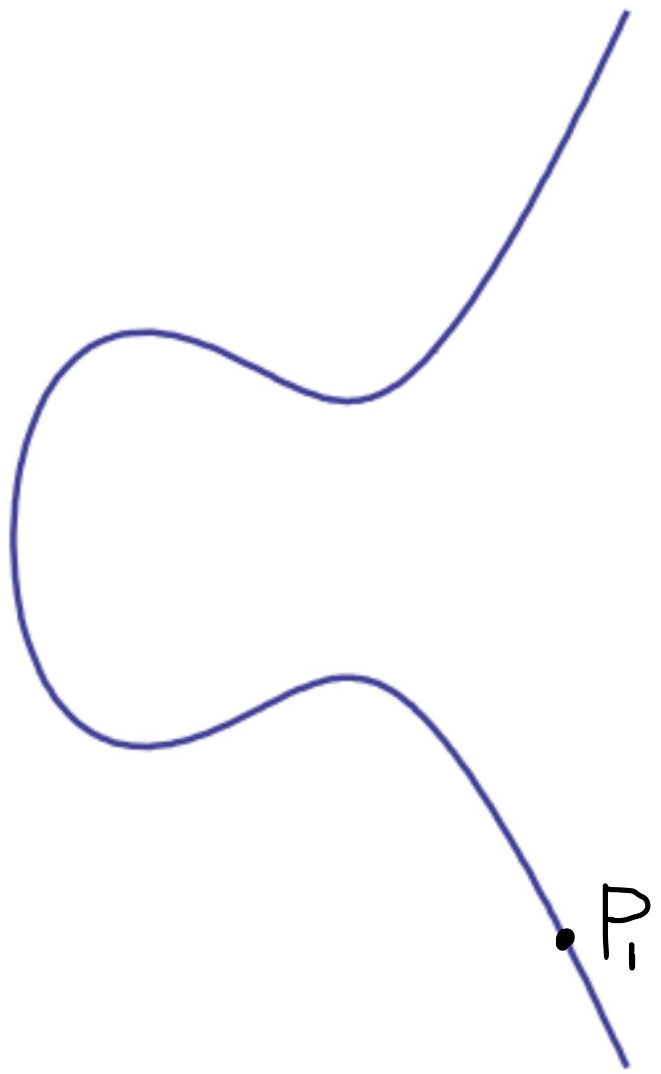
Given 2 generic points $\boldsymbol{u}, \boldsymbol{v}$, there is a 3rd point $\boldsymbol{w} = \boldsymbol{u} * \boldsymbol{v}$ such that $\phi(\boldsymbol{u}, \boldsymbol{v}, .) \sim \phi(\boldsymbol{u}, \boldsymbol{w}, .) \sim \phi(\boldsymbol{v}, \boldsymbol{w}, .)$

Pick identity $\boldsymbol{o}$, then group law is

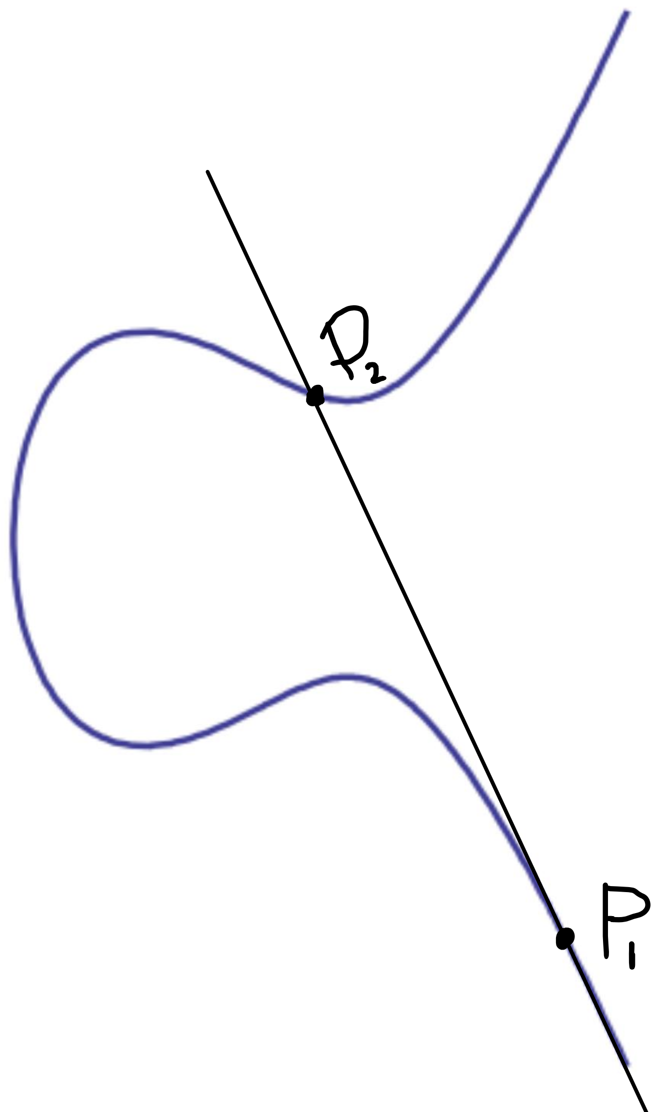
$$\boldsymbol{u} + \boldsymbol{v} \coloneqq \boldsymbol{o} * (\boldsymbol{u} * \boldsymbol{v})$$

Unfortunately we don't have an obvious point to use as identity.

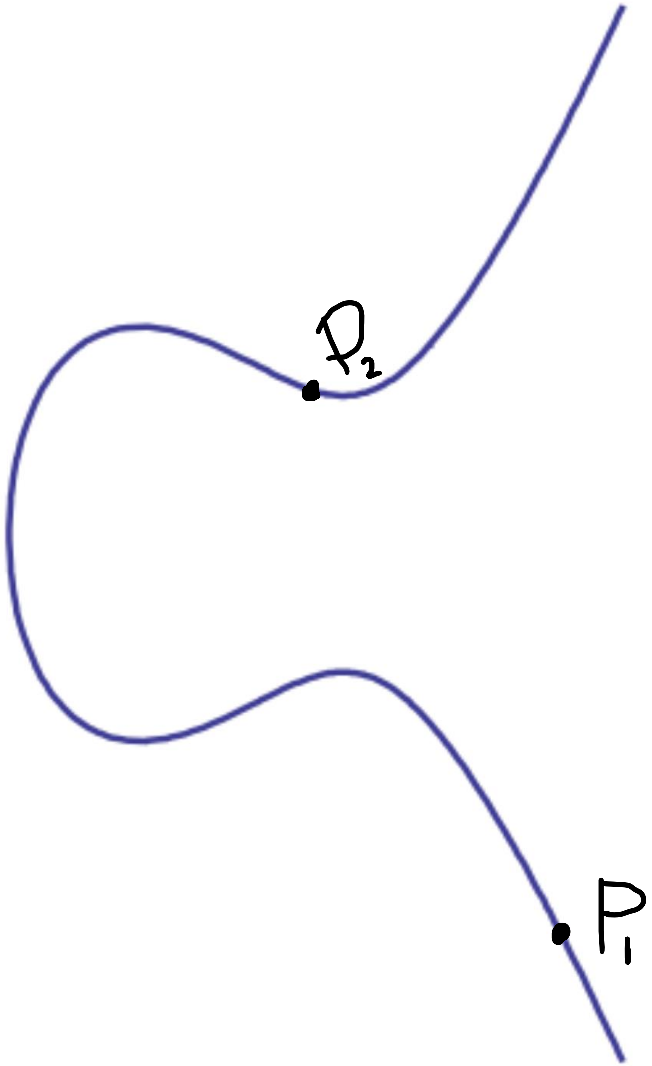
Canonically generating a 2nd point



Canonically generating a 2nd point



Canonically generating a 2nd point



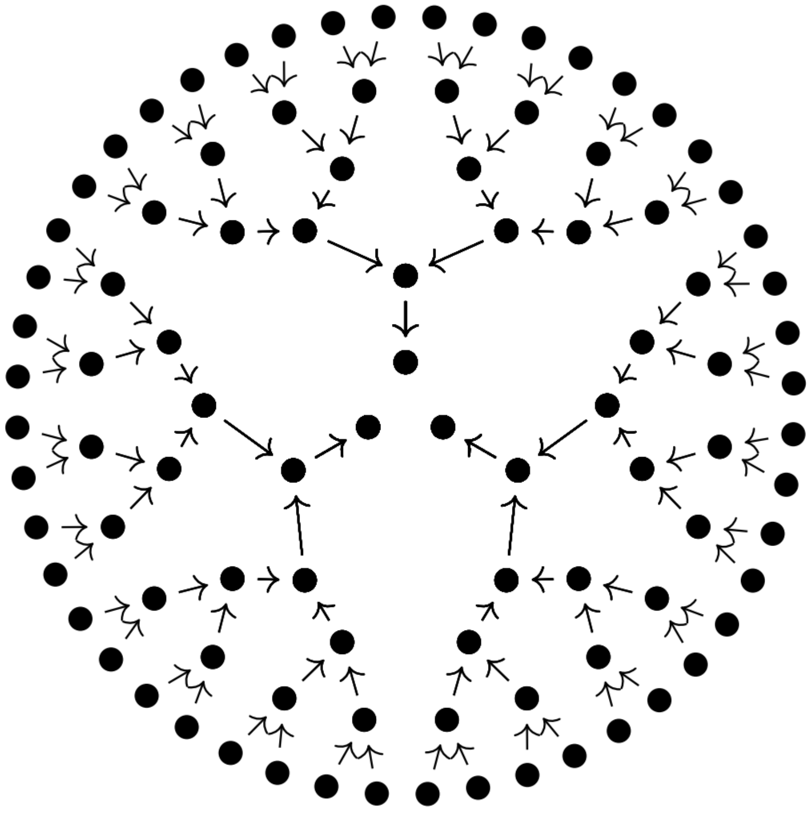
We have something analogous in the ATF world:

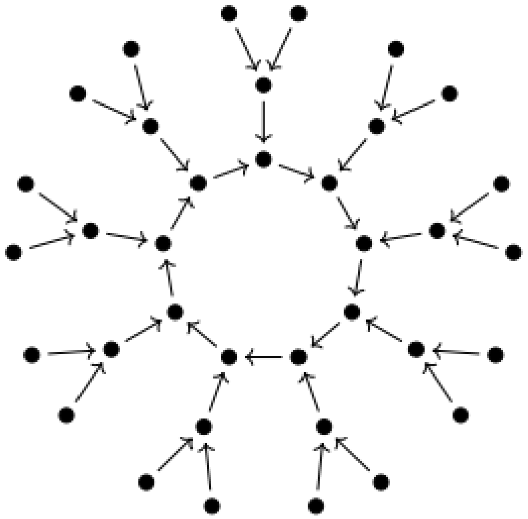
An efficiently computable function H that maps the set of rank-4 projective points to itself.

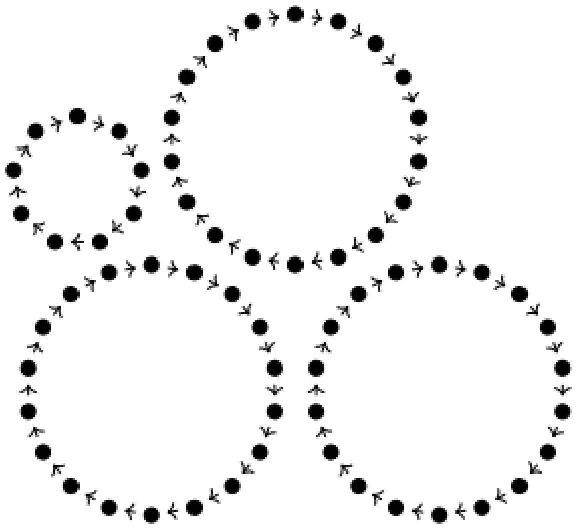
Iterating the function H gives a sequence of rank-4 points.

Graphs for the H-function

- Nodes are points of rank 4
- $\boldsymbol{u} \to \boldsymbol{v}$ if $H(\boldsymbol{u}) = \boldsymbol{v}$





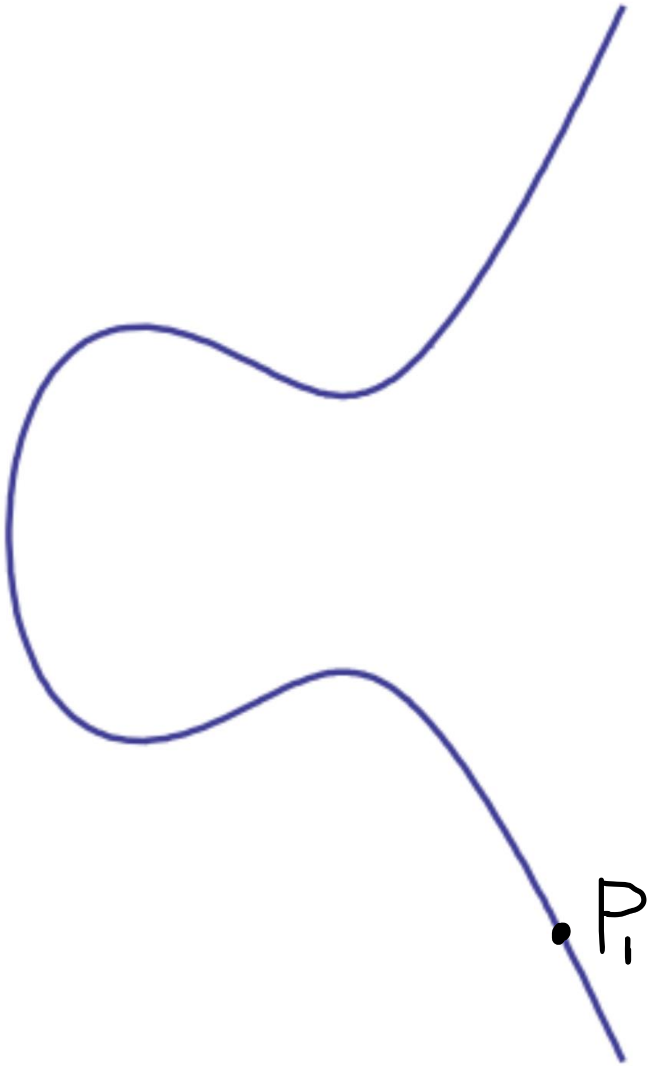


Attempt 2: Iterating H

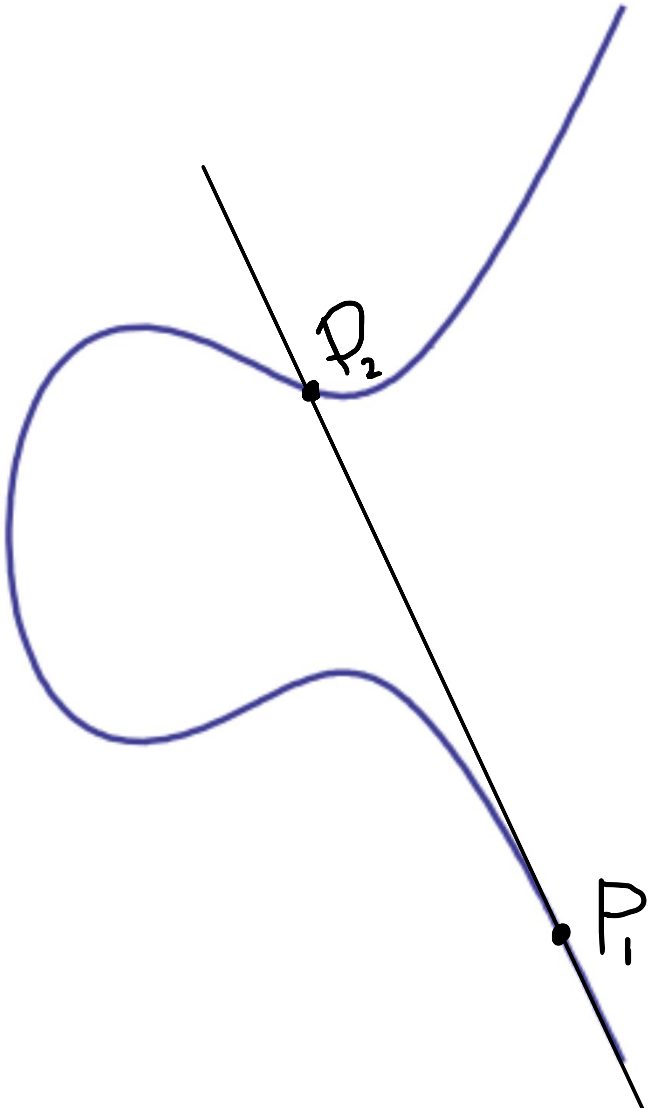
Given ϕ, u compute:

$$\boldsymbol{u}_1 = \boldsymbol{u}, \boldsymbol{u}_1 = H(\boldsymbol{u}_0), \ldots, \boldsymbol{u}_{11} = H(\boldsymbol{u}_{10})$$

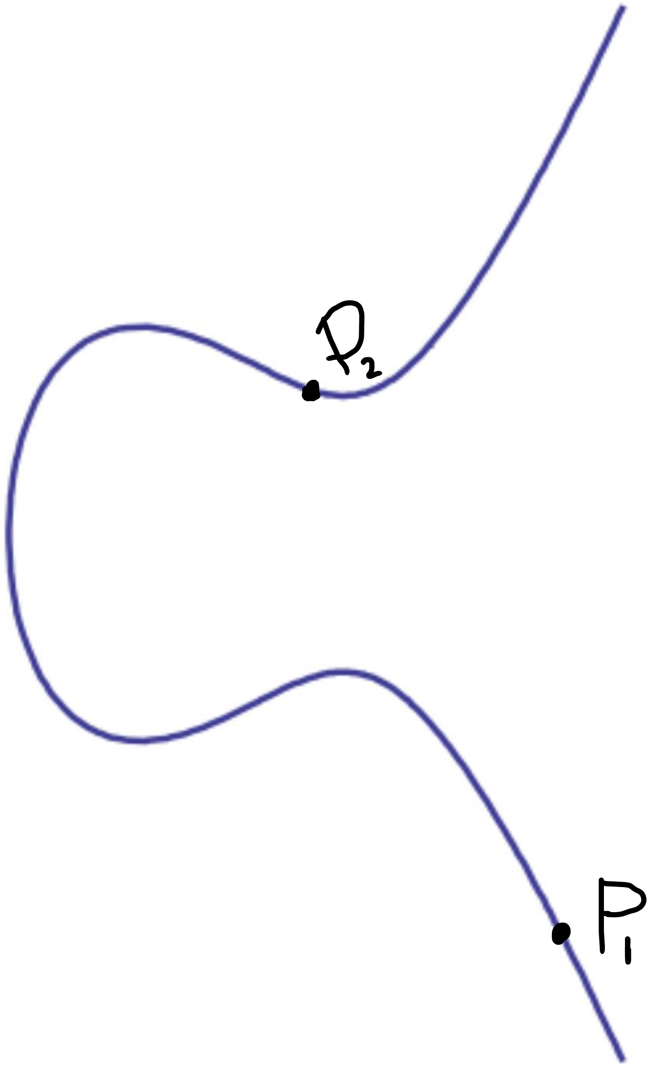
Generating a sequence of points



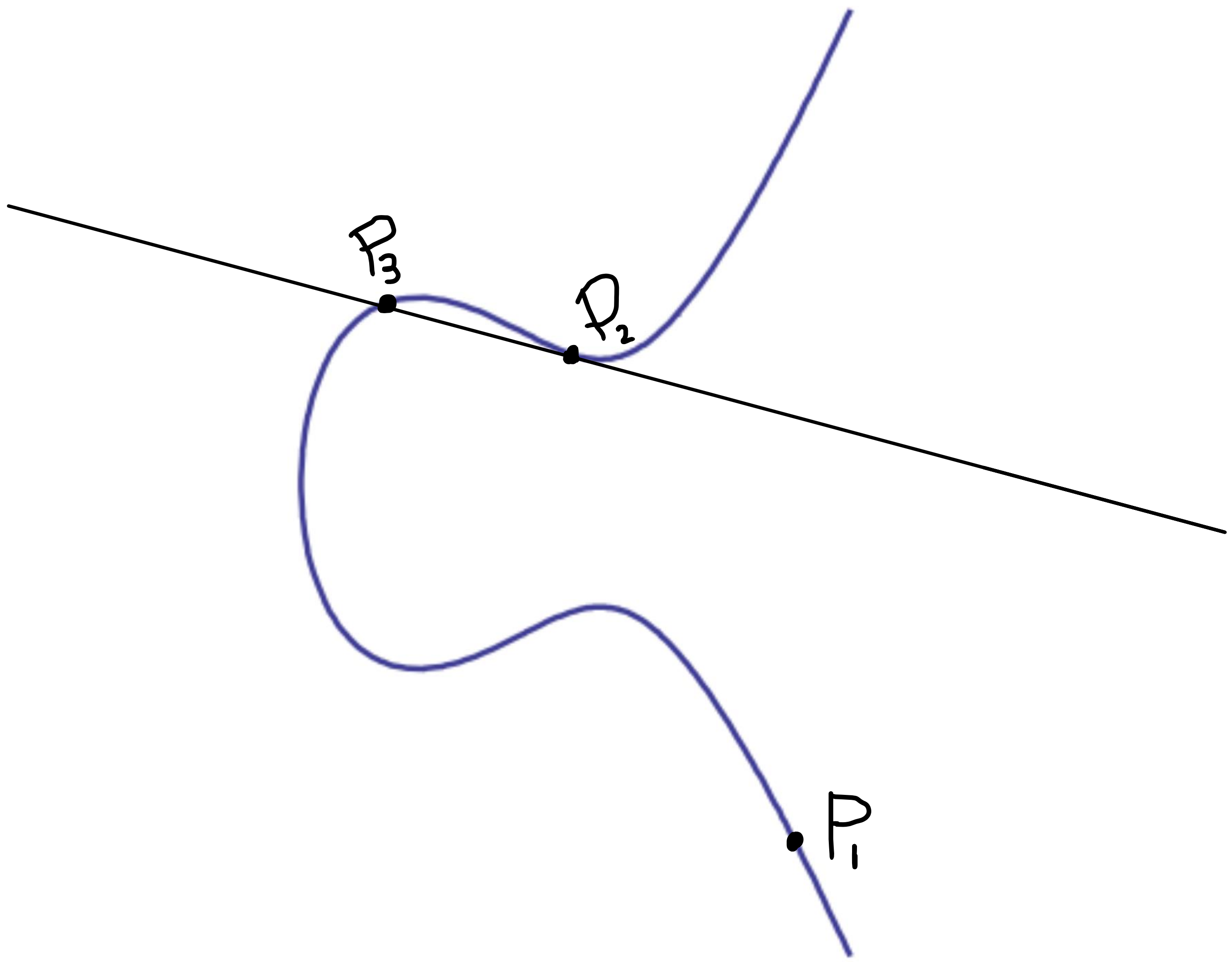
Generating a sequence of points



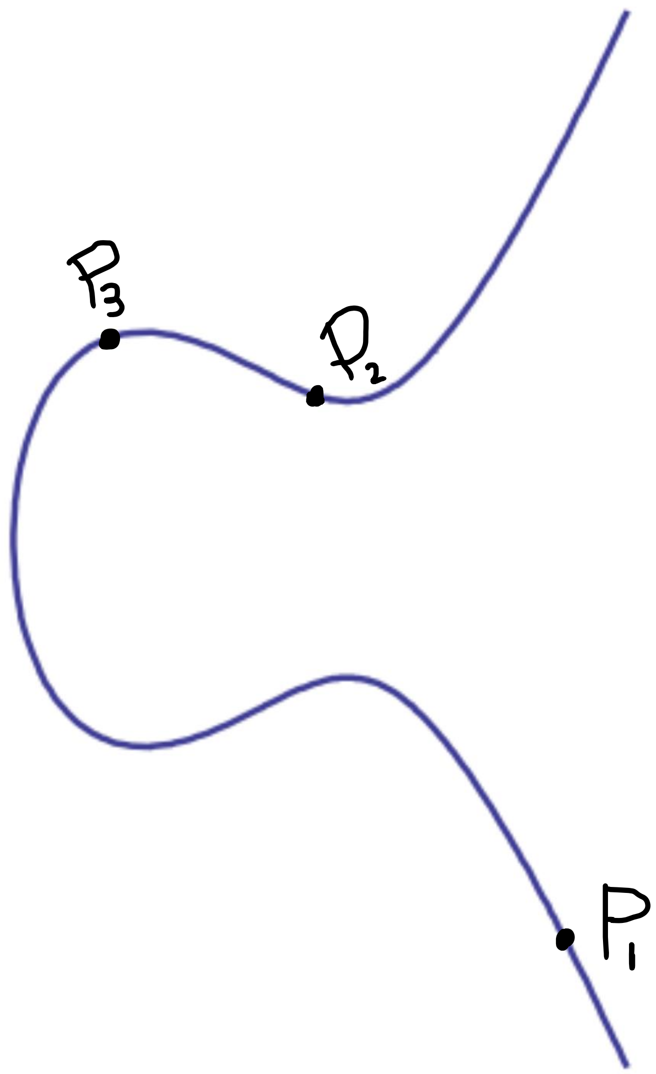
Generating a sequence of points



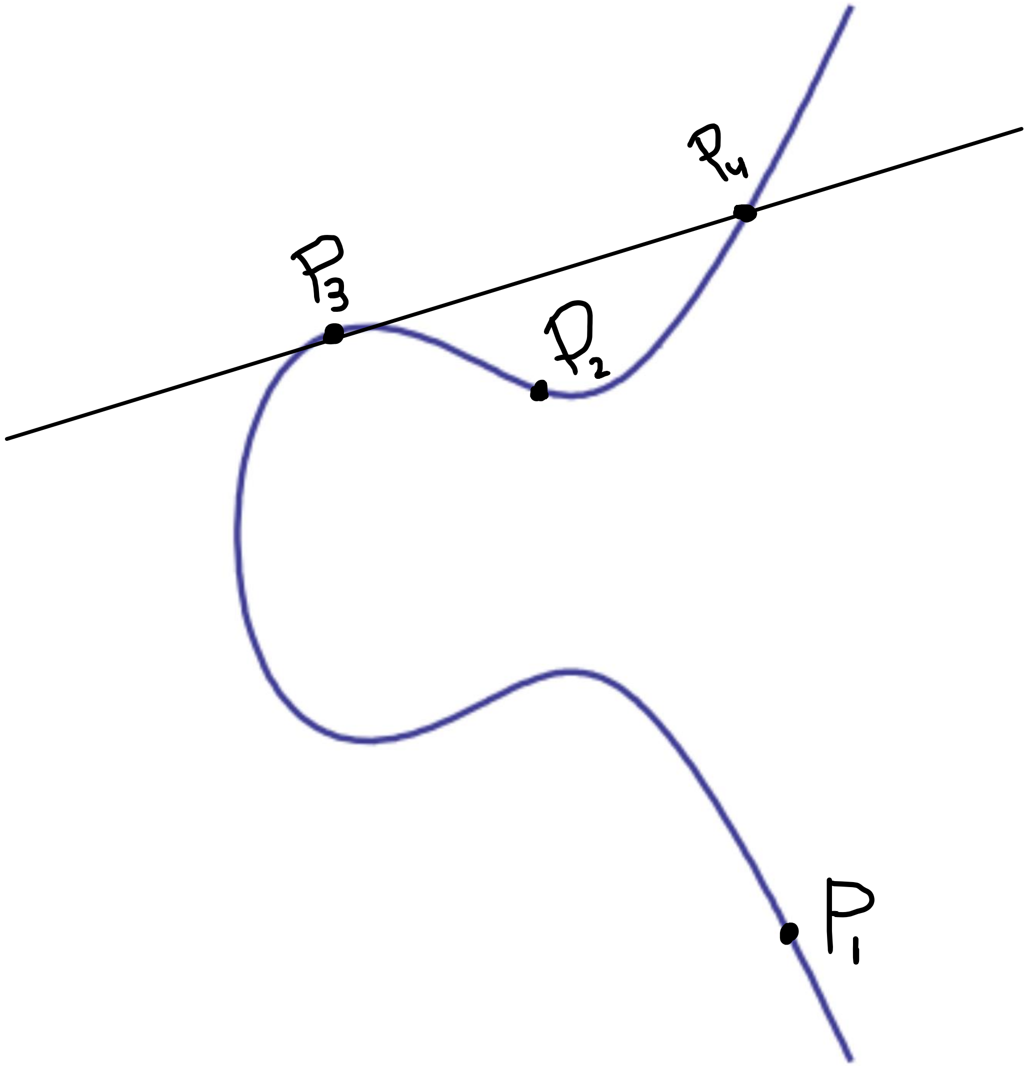
Generating a sequence of points



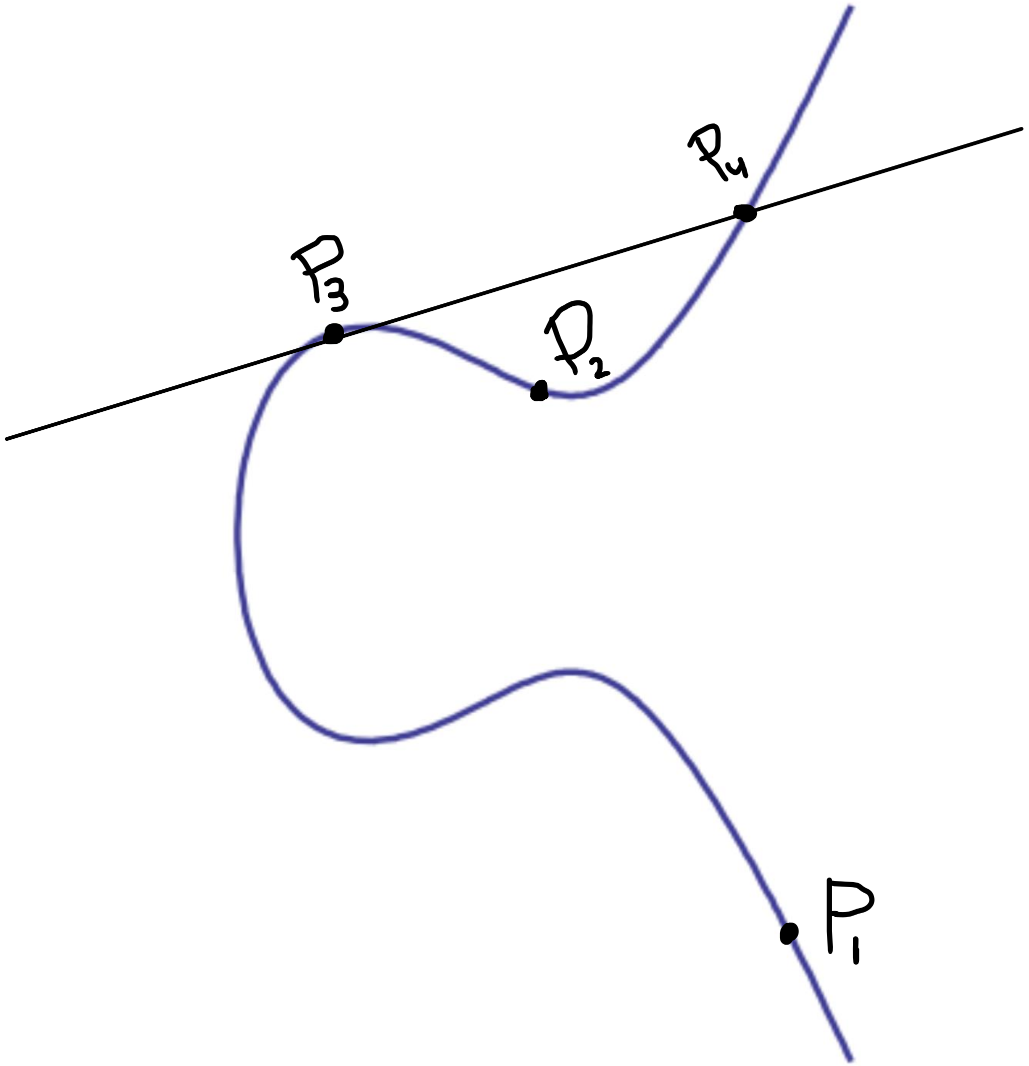
Generating a sequence of points



Generating a sequence of points



Generating a sequence of points



Attempt 2: Iterating H

Given ϕ, u compute:

$$\boldsymbol{u}_1 = \boldsymbol{u}, \boldsymbol{u}_1 = H(\boldsymbol{u}_0), \dots, \boldsymbol{u}_{11} = H(\boldsymbol{u}_{10})$$

With high likelihood $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_{10}]$ forms a projective frame, so we can write $\boldsymbol{u}_{11}$ uniquely as a combination $u_{11} = \sum \alpha_i u_i$, with α_i unique up to multiplication by a scalar.

We define $F(\phi, u) = (\alpha_i)_{i \in [10]}$, such that $\boldsymbol{u}_{11} = \sum \alpha_i \boldsymbol{u}_i$.

Experiments suggest this is a perfect invariant i.e. $F(\phi_1, u) = F(\phi_2, v)$ if and only if there is $S \in GL(V)$ with

$$\phi_2 = \phi_1 \circ S \text{ and } u = Sv.$$

Algorithm for solving ATFE problem:

1) Sample $O(q)$ rank-4 points for ϕ_1 and ϕ_2 and compute the invariants.
2) When a collision $F(\phi_1, u) = F(\phi_2, v)$ recover S from the canonical frames.

Heuristically, the complexity is $O(q)$.

In practice the algorithm takes between 30 minutes and 4 hours for the $(n = 9, q \approx 2^{19})$ parameters.

Conclusion:

- Original parameters for ATFE problem are too small (NIST submission has 16KB sigs vs 5KB of earlier version)

Open questions:

- Does the attack for $n = 9$ generalize to higher n?
- Finding better attacks for large n
- Can we use the ATF torsors constructively?
- ...