Sleeping in the volcano

ECC Rump Session

Damien Robert

(Slides done under pressure by Ben looking for guinea pigs for the xtomato program)

19/09/2011 (Nancy)

Sleep sort

- New breakthrough algorithm for sorting a list of integers.

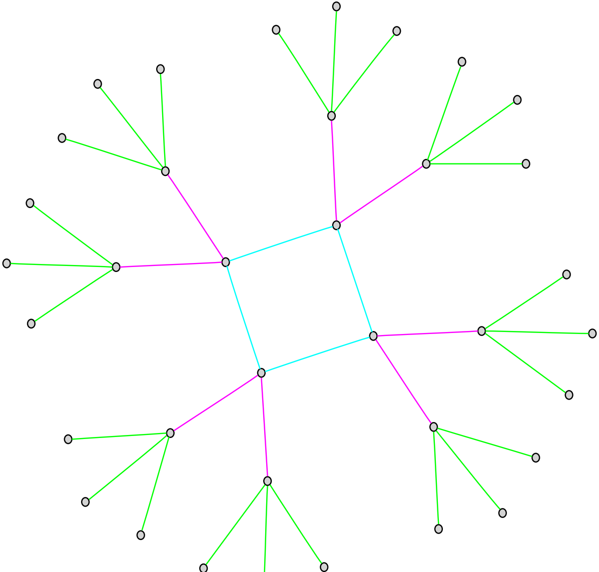
  ```
  #!/bin/sh

  for i in ”$@”; do
    ( sleep ”$i”; echo ”$i” ) &
  done

  wait
  ```

  Source: Anonymous from 4chan, http://dis.4chan.org/read/prog/1295544154.

- Linear in the size of the biggest integer! This is clearly better than the $O(n \log n)$ stuff.
- How to apply this idea to ECC? I like isogenies....

Isogeny volcano and cryptography

- The graph of ℓ-isogenies from an elliptic curve form the structure of a volcano [Kohel, Fouquet-Morain]:

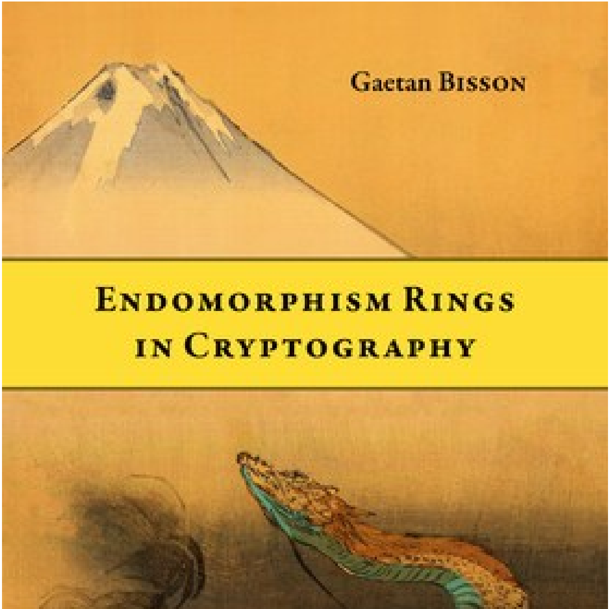


Isogeny volcano and cryptography

- Lots of cryptographic applications: a search on google scholar for “volcano cryptography” yields 341 results. A search for “elliptic curve cryptography” (In Russian: “криптографии на эллиптических кривых”) yields only 286 results.
- It is a well known method of attacks: “Look at this nice volcano!”, to distract the opponent to steal his secret key.

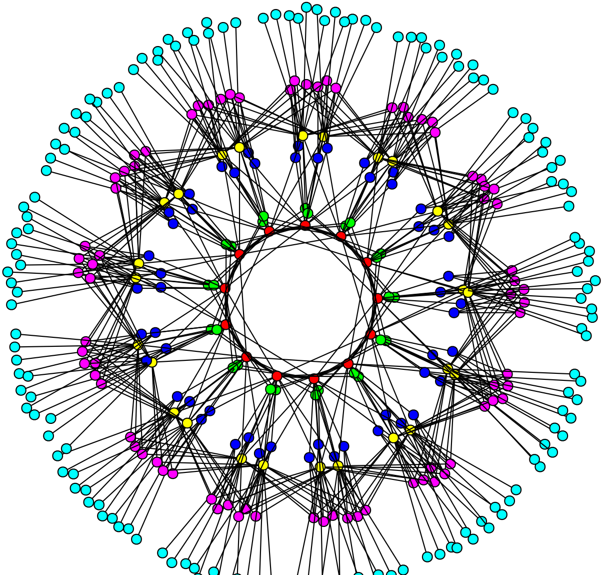
Isogeny volcano and cryptography

- Can even be used to get a phd thesis:



Isogeny volcano and cryptography

- Beware of false volcanoes (coming from the evil dimension 2 case)



A little publicity between two tomatos

How was the previous isogeny graph in dimension 2 computed?

With AVIsogenies (Abelian varieties and isogenies) a powerful, efficient, fast and bug free (someday) Magma package for the algorithmic of abelian varieties!

You can find it with all good browsers on
`http://avisogenies.gforge.inria.fr`.
Current release: 0.5.

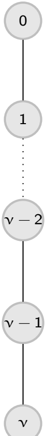
Developed by Bisson , Cosset and Robert.

Since last year ECC's rump session: complete addition law, isogenies in characteristic 2, faster endomorphism ring computation and bugs fixes.

This slide is protected by "**ouch my eyes!**" technology. To make it difficult to copy this slide, the colors change with each compilation.

Exploring the structure of the volcano

- If E is on the floor, then $E[\ell^\infty](\mathbb{F}_q)$ is cyclic: $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^m\mathbb{Z}$ (possibly $m = 0$).
- If E is on level $\alpha < m/2$ above the floor, then $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^\alpha \oplus \mathbb{Z}/\ell^{m-\alpha}$.
- If E is on level $\alpha \geqslant m/2$, then m is even and $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2} \oplus \mathbb{Z}/\ell^{m/2}$.



$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m/2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m/2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m/2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{2}\mathbb{Z} \oplus \mathbb{Z}/\ell^{m-2}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell^{m-1}\mathbb{Z}$

$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{m}\mathbb{Z}$

Walking on the isogeny volcano

From the list of curves in the isogeny graph, sort them according to their level in the volcano:

```
function sleep_walk(elliptic_list,l)
  E:=Rep(elliptic_list);
  n:=#E;
  nu:=Valuation(n,l);
  gamma:=n div l^nu;
  function highest_point(E)
    P:=gamma*Random(E);
    for i in [nu div 2..nu] do
      if P eq E!0 then return i; end if;
      P:=l*P;
    end for;
  end function;
  for E in elliptic_list do
    j:=jInvariant(E);
    depth:=highest_point(E);
    command:=Sprintf(”sh -c \”( echo \\\”%o\\\” ; sleep \\\”%o\\\”)&\””,
      j, depth);
    system(command);
  end for
end function
```

Q & A

The above program is bug free and always work except when it does not.

- Q: Sometimes curves on different levels are outputted at the same time.
  A: You have a non regular volcano. Please don't apply the algorithm to these volcanoes
- Q: Sometimes highestpoint does not output the right answer.
  A: Suppose that $E[\ell^\infty] =< P, Q >$ with $\text{ord}(P) \mid \text{ord}(Q)$. This situation happen when the random point $R = \alpha P + \beta Q$ computed is such that $\ell \mid \beta$. Increasing ℓ should reduce the probability of this.
- Q: If there is too many curves, the results are not sorted in the right order.
  A: Buy a faster computer. Or change the value in the sleep function.

Next year: climbing a (real) volcano