Breaking D.L. at Mont Saint-Michel

Pierre KARPMAN

Brice MINAUD

Alex WALLET

Staff \o/

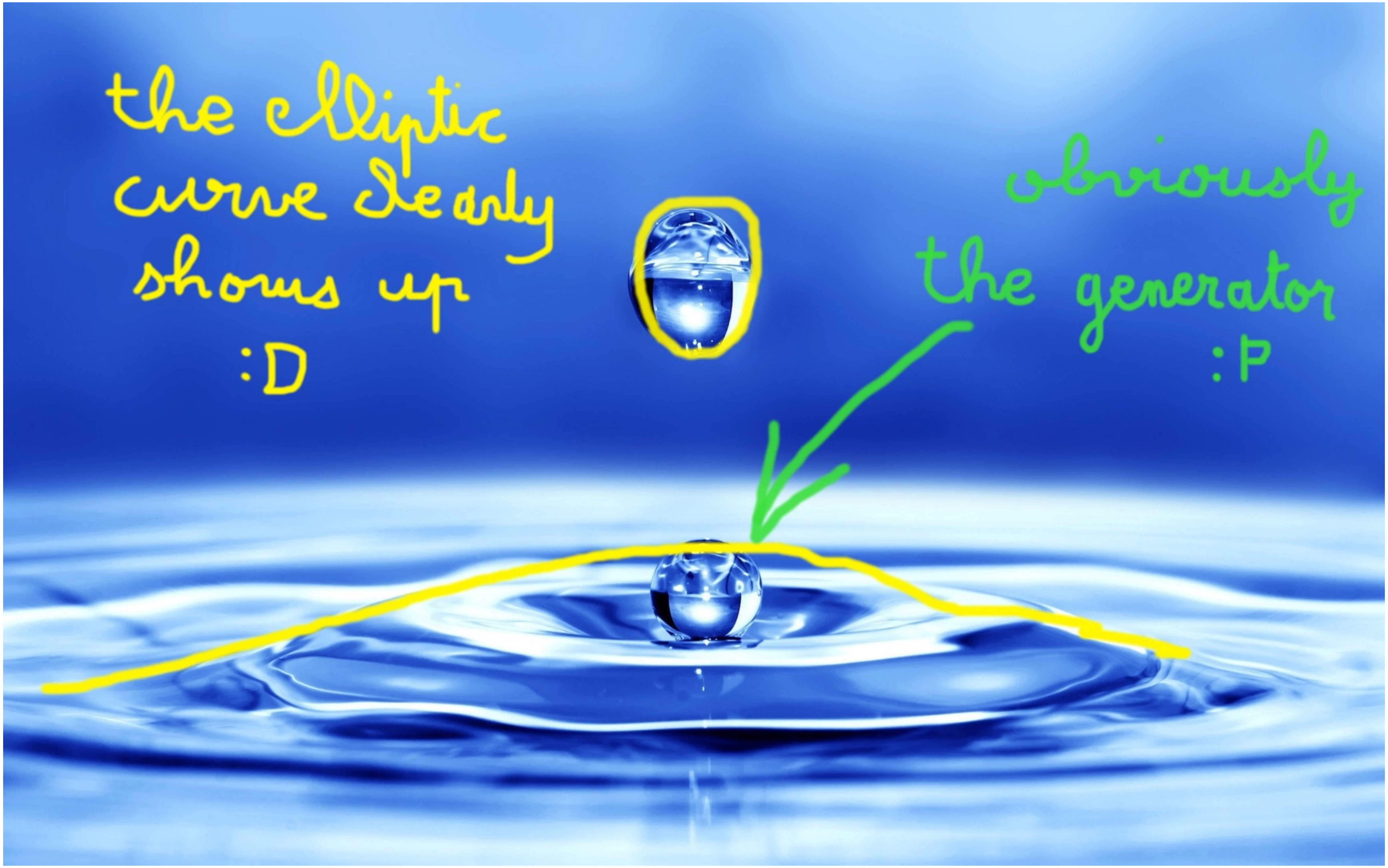
What is an elliptic curve?

this is
an elliptic
curve
:)

A Physical Model for Elliptic Curves

A Physical Model for Elliptic Curves

A Physical Model for Elliptic Curves



How to use that in crypto?

?

:/

Cloud Power!!

Parallelization!!!!!

Pros & Cons

Pros

100% **green** crypto attack

Bye-bye point counting!

Works well up to countably infinite number #points (roughly)

Cons

Only works well in Brittany (or rainy places…)

Results

groups 1,2,3,4 yesterday X(

Results

4 NIST curves broken in 15 minutes XD

Perspectives

- Get more computing power (e.g. privatize UK…)
- Badly need a Photoshop license :’(

Merci