An ECG for Christmas

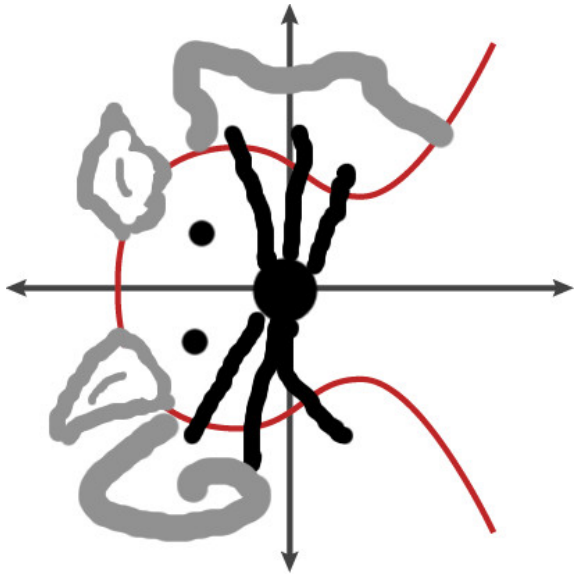
Jean-Pierre Flori, Jérôme Plût, Jean-René Reinhard

Agence nationale de la sécurité des sytèmes d'information

September 28, 2015

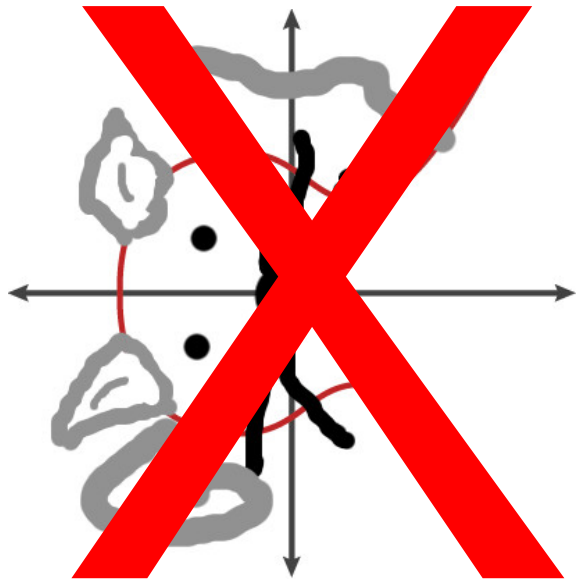
But what is an ECG?

An Elliptic Cat Generator?

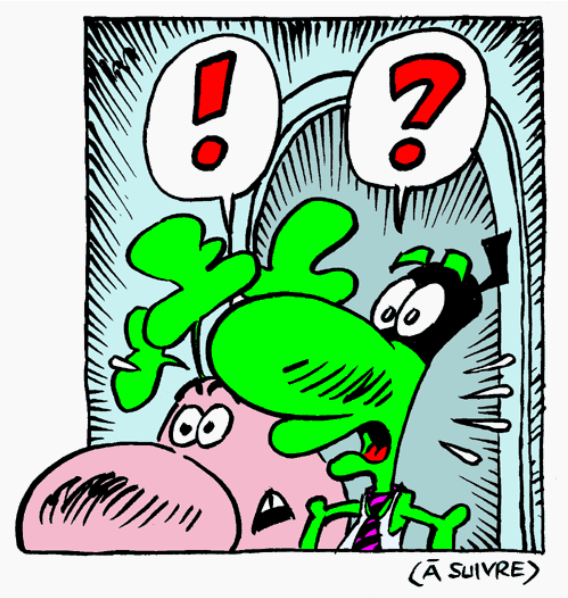


An Elliptic Cat Generator?

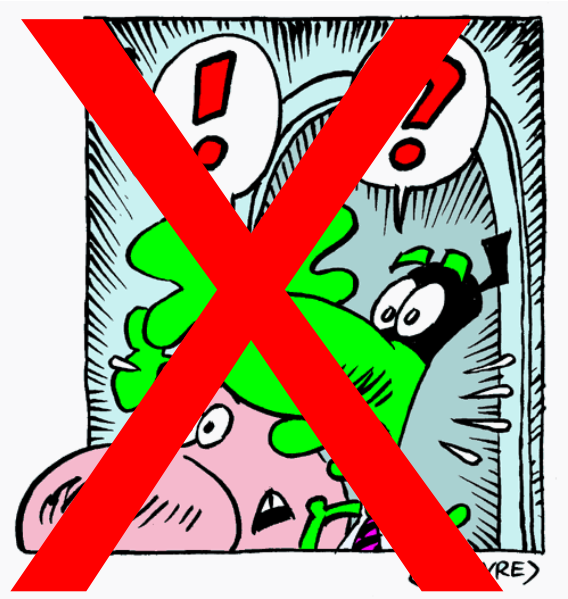
NO!



An Exceptional Cucumber Gardener?



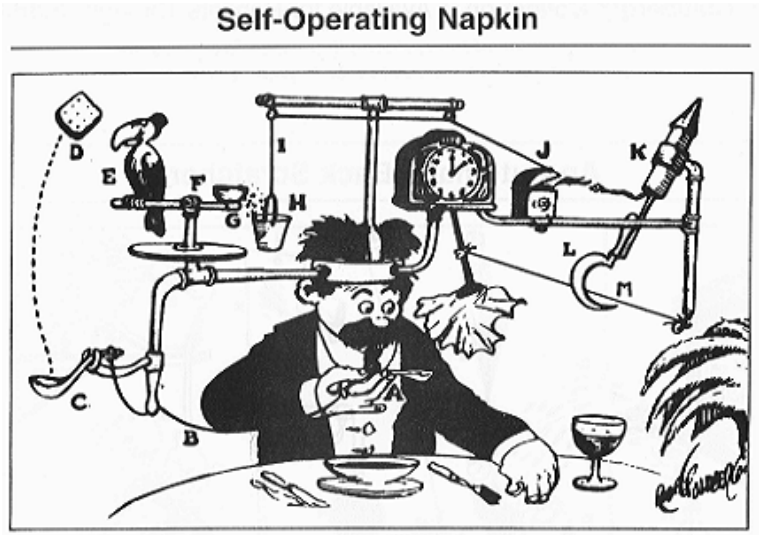
An Exceptional Cucumber Gardener?



NO!

An Extraordinary Complicated Gadget?

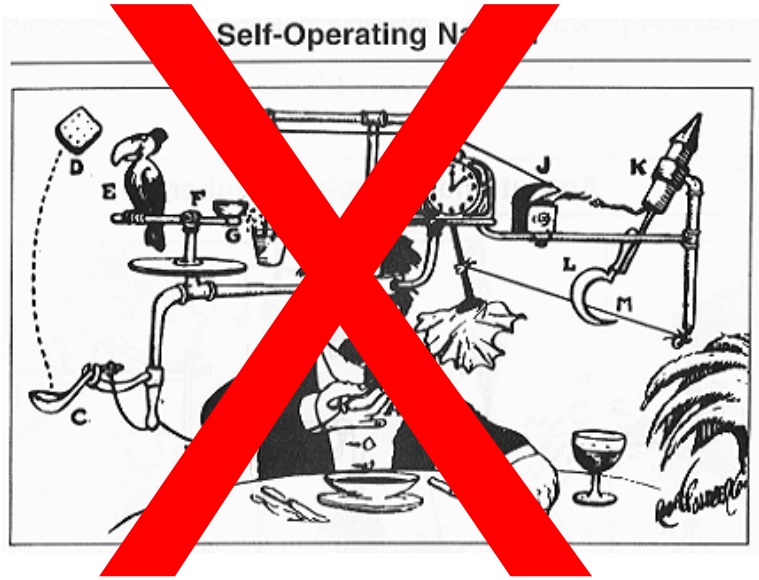
x



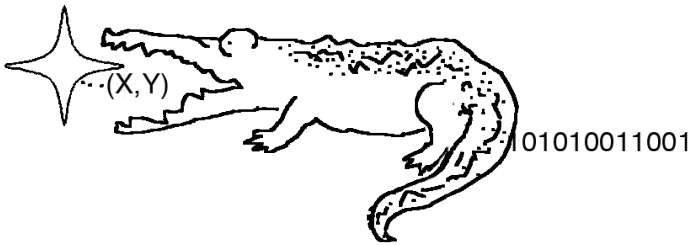
An Extraordinary Complicated Gadget?

x

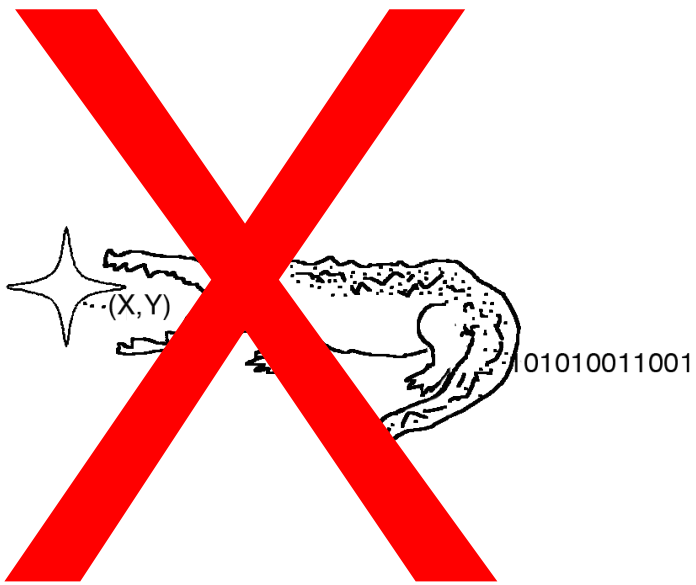
NO!



An Elligator Curve Generator?



An Elligator Curve Generator?



NO!

An Exciting Christmas Gift?

An Exciting Christmas Gift?

Maybe. . .

An Elliptic Curve Generator?

An Elliptic Curve Generator?

YES!

But what for?

But what for?

Generate curves for crypto together with certificates!

```
sage: ECG.generate_curve() [ENTER]
```

Curve

```
(2017, -3, 625)
order = 2063, point = (0, 25)
twist_order = 1973
disc_factors = {6043}
class_number = 9, form = (17,3,89)
embedding_degree = 1031, factors = {2, 1031}
twist_embedding_degree = 493, factors = {2, 17, 29}
```

Rejected curves

```
((2017, -3, 5), composite, 2065, witness, 1679, point, (1,258))
((2017, -3, 25), torsion_point, 3, point, (448, 288))
((2017, -3, 125), torsion_point, 2, point, (982, 0))
```

Powered by Sage(math), PARI/GP, ...

Coming for Christmas.

Coming for Christmas.

(Somewhere on the internet.)