Discovering new ways of attacking AES when trying to do something else

Martin Grenouilloux
<martin.grenouilloux@lse.epita.fr>

Algebraic cryptanalysis: Optimization of Gröbner basis against AES-128

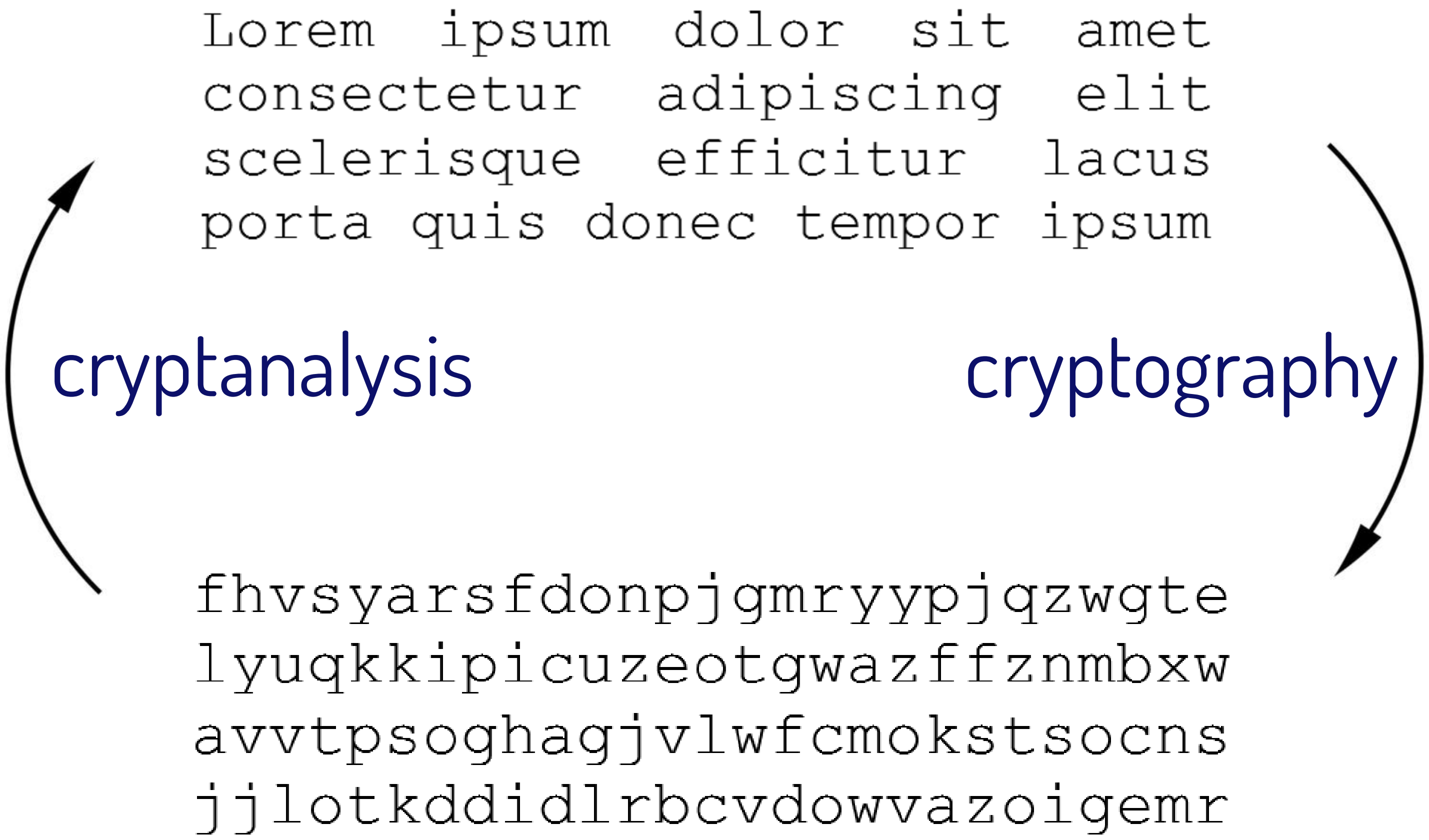
Algebraic cryptanalysis: Optimization of Gröbner basis against AES-128

Algebraic cryptanalysis: Optimization of Gröbner basis against AES-128

Algebraic cryptanalysis: Optimization of Gröbner basis against AES-128

What is algebraic cryptanalysis ?

Cryptography, Cryptanalysis ...



Lorem ipsum dolor sit amet
consectetur adipiscing elit
scelerisque efficitur lacus
porta quis donec tempor ipsum

cryptanalysis

cryptography

fhvsyarsfdonpjgmryypjqzwgte
lyuqkkipicuzeotgwazffznmbxw
avvtpsoghagjvlwfcmokstsocns
jjlotkddidlrbcvdowvazoigemr

Cryptography, Cryptanalysis ...

$$\underbrace{\text{cryptanalysis} \quad + \quad \text{cryptography}}_{\text{cryptology}}$$

Algebraic cryptanalysis ?

- Breaking codes by solving polynomial systems of equations

$$\begin{cases} aX^7 + bX^4 + cX^2 + d = 0 \\ cX^6 + dX^2 + aX + b = 0 \\ aX^4 + cX^3 + dX + e = 0 \end{cases}$$

What is AES ?

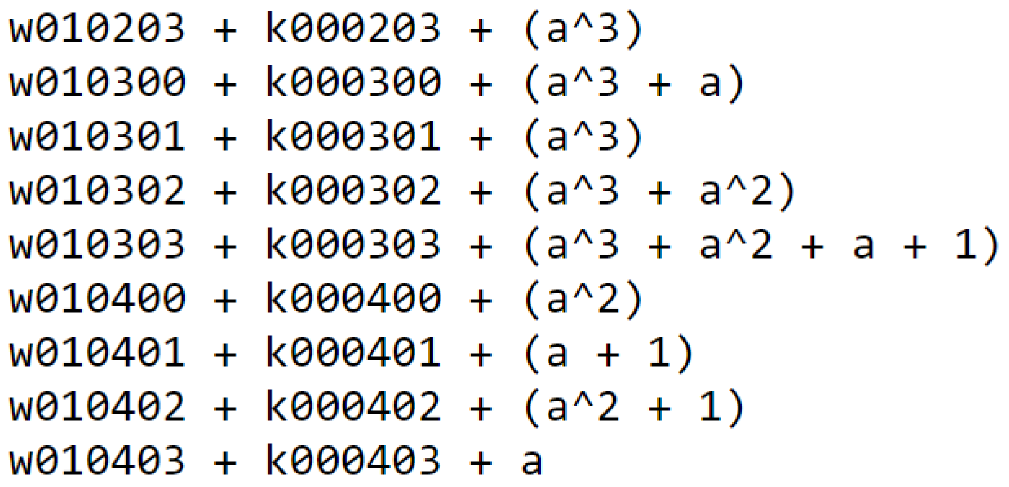
Advanced Encryption Standard

- Symmetric encryption
  - key size: 128, 192 or 256*

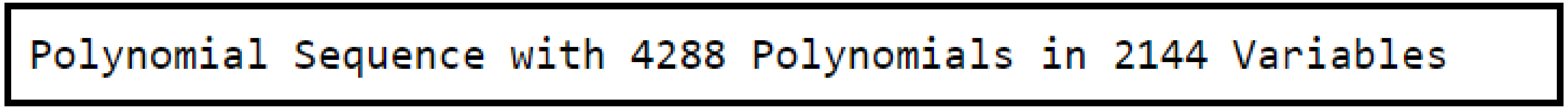
- Provides confusion and diffusion
  - bits of plaintext depend on different bits of the key
  - avalanche effect

AES seen differently

We use this property to study encryption as a system of polynomials



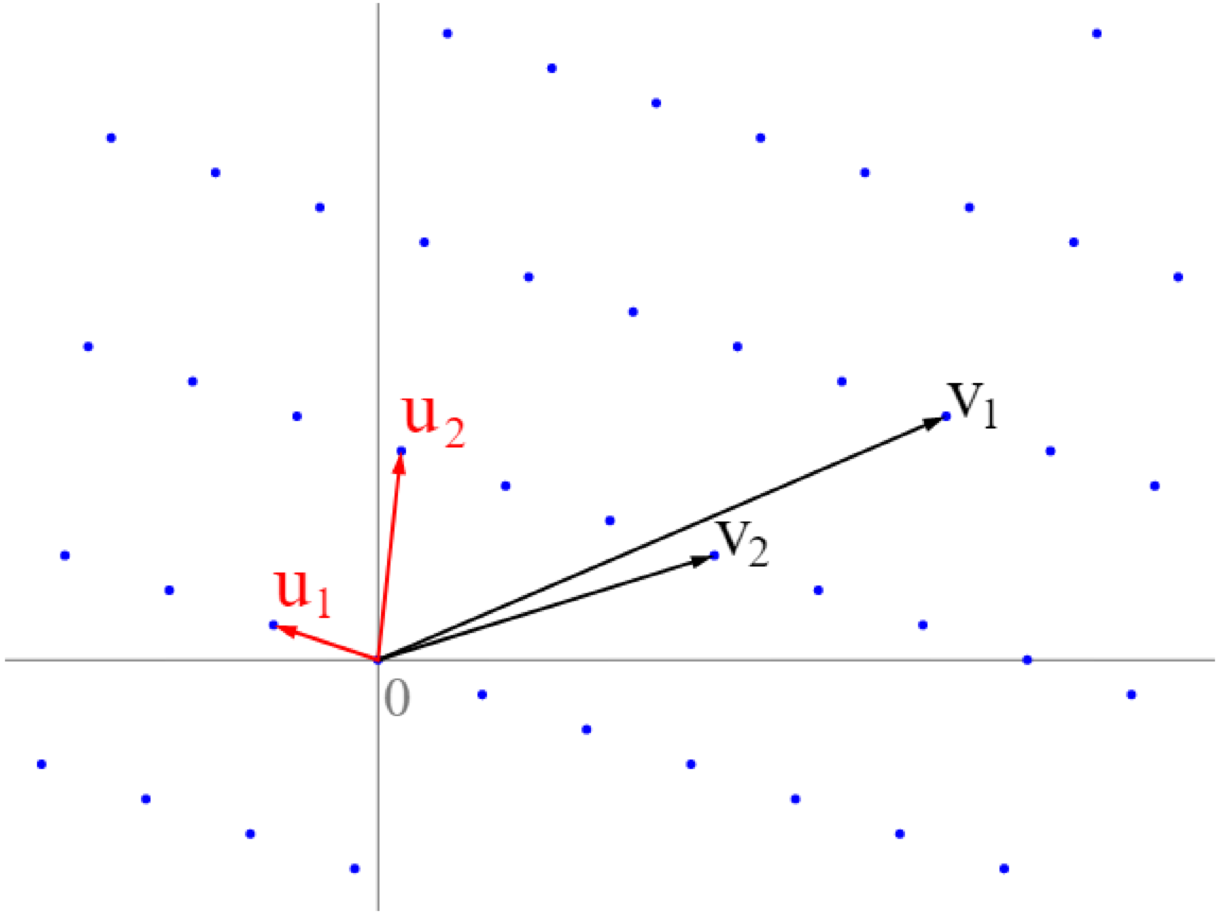
```
w010203 + k000203 + (a^3)
w010300 + k000300 + (a^3 + a)
w010301 + k000301 + (a^3)
w010302 + k000302 + (a^3 + a^2)
w010303 + k000303 + (a^3 + a^2 + a + 1)
w010400 + k000400 + (a^2)
w010401 + k000401 + (a + 1)
w010402 + k000402 + (a^2 + 1)
w010403 + k000403 + a
```



```
Polynomial Sequence with 4288 Polynomials in 2144 Variables
```

What are Gröbner basis ?

About bases



A cool way to deal with polynomial rings

A basis that generates for all polynomials of its ring's ideal

Change from the study of polynomials to the study of monomials

Computing a Groebner basis of AES is almost the same as retrieving the key and plaintext

A slow way to deal with polynomial rings

Computing such a basis is hard

Hence our will to optimize it;

- Gaussian elimination & matrix triangulation
- Degree order ?
- Separation into independent systems

A graphical way to deal with polynomial rings

Verify it mathematically (lame)

Transform the system into a graph (stylish)

$$\begin{cases} aX^7 + bX^4 + cX^2 + d = 0 \\ cX^6 + dX^2 + aX + b = 0 \\ aX^4 + cX^3 + dX + e = 0 \end{cases}$$

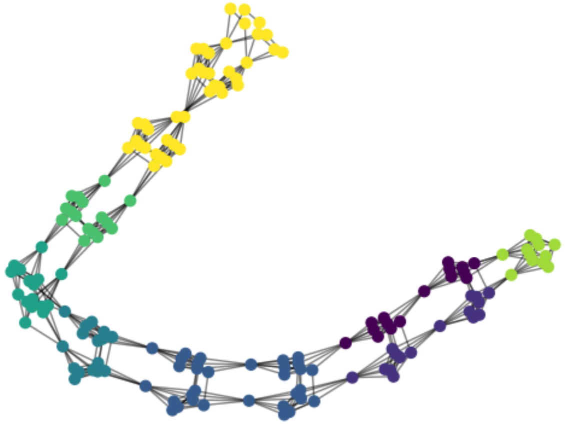
e depends on a, c and d

a depends on b, c, d and e

A graphical way to deal with polynomial rings

Verify it mathematically (lame)

Transform the system into a graph (stylish)

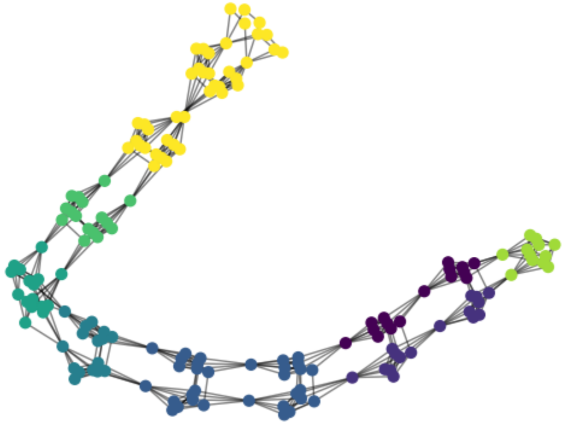


Only one system of equations

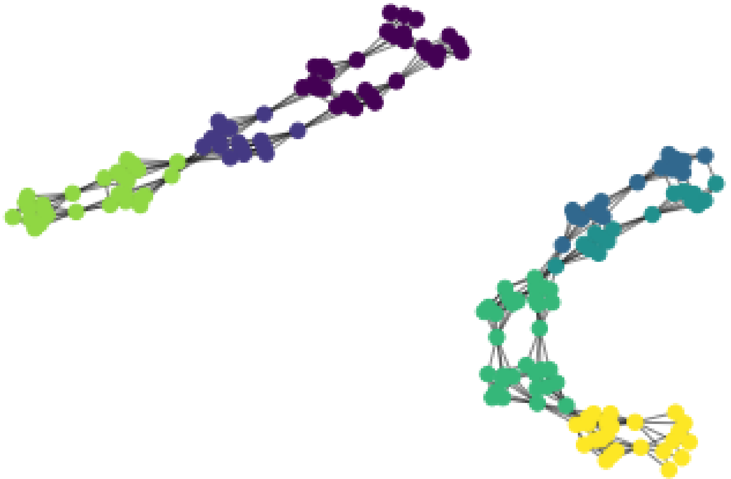
A graphical way to deal with polynomial rings

Verify it mathematically (lame)

Transform the system into a graph (stylish)



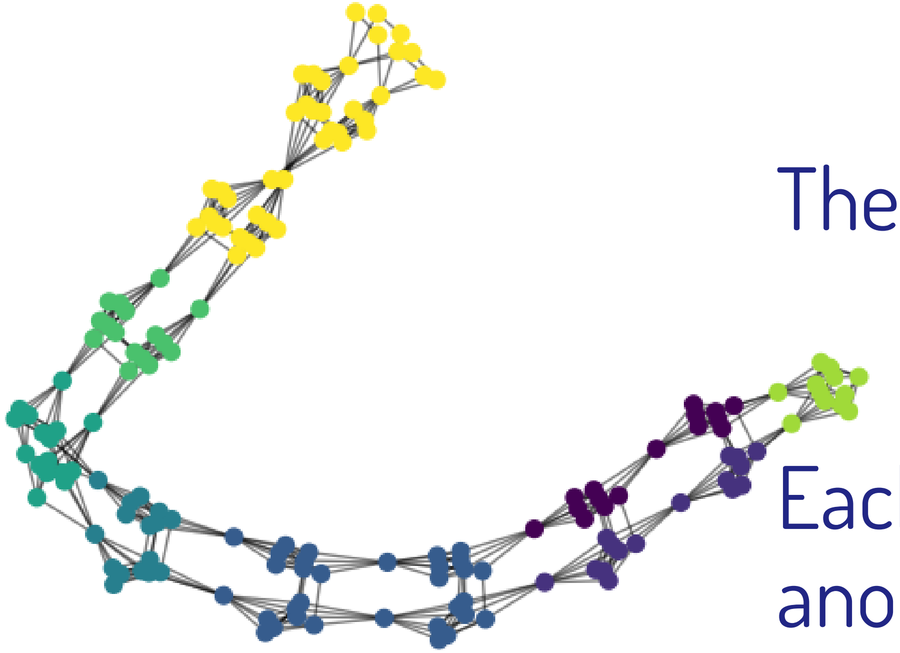
Only one system
of equations



Two systems linearly
independent

Cool bro, now what ?

AES graphs in a nutshell

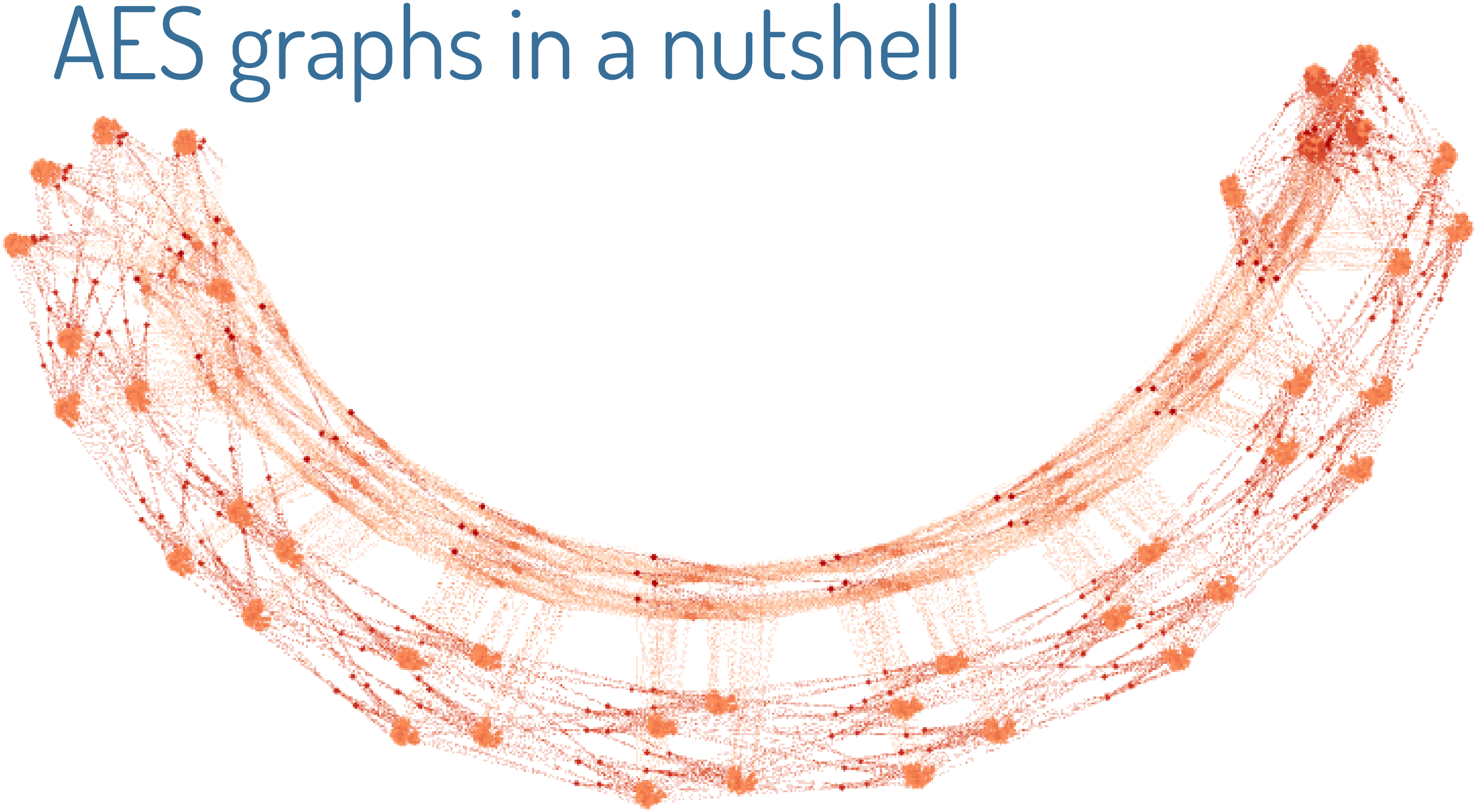


They present distinct communities

Each community is bound to another by a few nodes

This trend goes chaotic with the number of rounds in AES

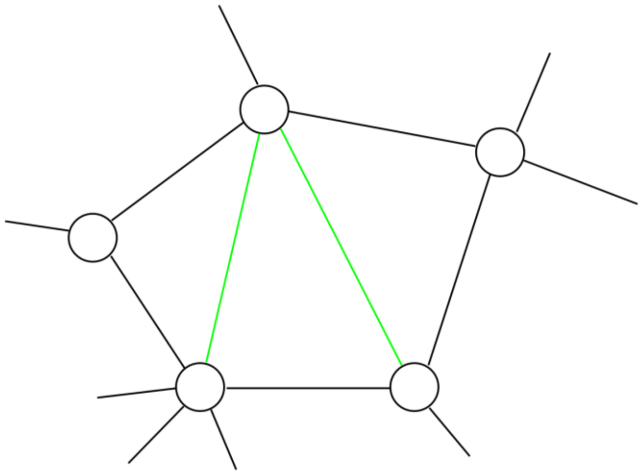
AES graphs in a nutshell



Graph example from AES 128 – 10 rounds

Chordal graphs

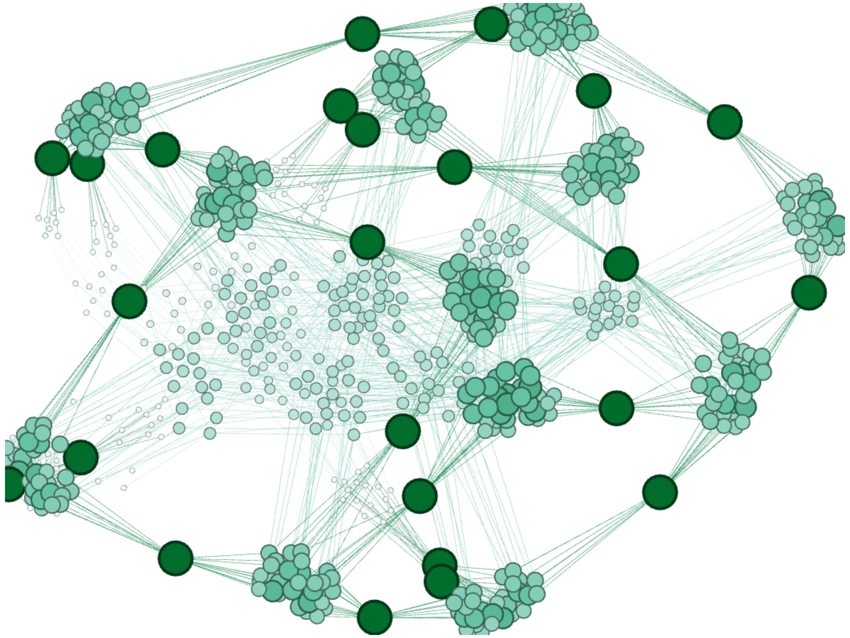
Chordal graphs



A graph in which all cycles of size 4+ have a chord

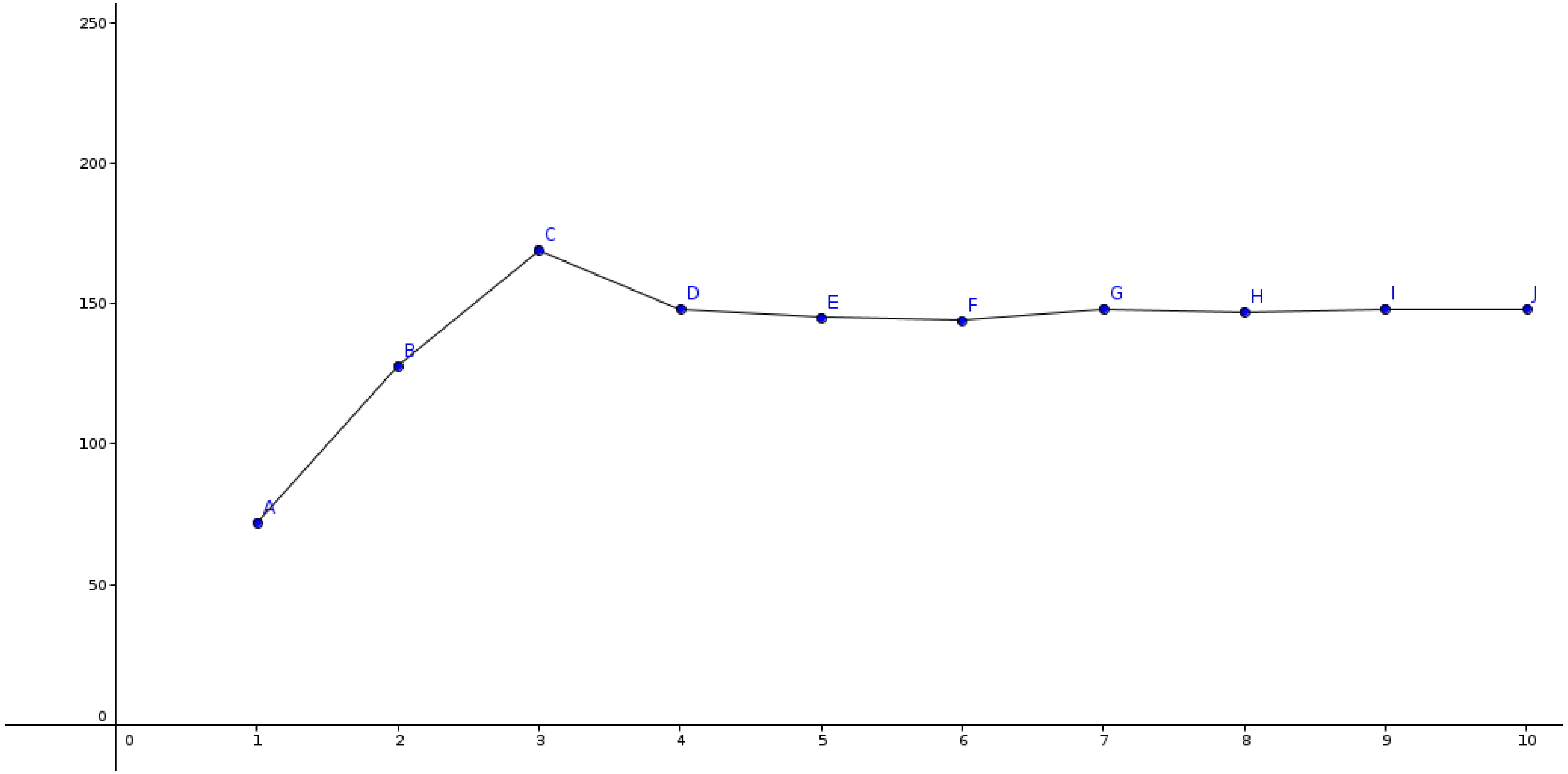
AES confusion property only create chordal graphs !

Proven resistant to sub-graph separation



2^140 complexity for AES128 – 10 rounds

Proven resistant to sub-graph separation



Minimum bitguessing for each round of AES128

Totally not what was planned

That's part of research !

Any questions ?

Martin Grenouilloux
<martin.grenouilloux@lse.epita.fr>

Algebraic Cryptanalysis
(Gregory V. Bard)

Algorithmic algebraic techniques and their application to block cipher cryptanalysis
(Martin Albrecht)