Hommage à Racine

Anne Canteaut

Inria, Paris, France

French Symmetric Encryption 2019, Paris

Jean Racine (1639-1699)

Jean Racine (1639-1699)

Pour qui sont ces SERPENT*s qui sifflent sur vos têtes ?*

In *Andromaque*

Jean Racine (1639-1699)

Pour qui sont ces RIJNDAEL *qui sifflent sur vos têtes ?*

In *Andromaque*

Jean Racine (1639-1699)

Pour qui sont ces XOODOO *qui sifflent sur vos têtes ?*

In *Andromaque*

A Tribute to Roots

Anne Canteaut

Inria, Paris, France

Fast Software Encryption 2019, Paris

Tragic Destiny of Roots

The importance of roots is underestimated...

- *The choice of the primitive root* $\boldsymbol{\alpha} \in \mathbb{F}_{\mathbf{2}^{n}}$ *does not matter*
- We often use irreducible polynomials...

Tragic Destiny of Roots

The importance of roots is underestimated...

- *The choice of the primitive root* $\alpha \in \mathbb{F}_{2^n}$ *does not matter*
- We often use irreducible polynomials...

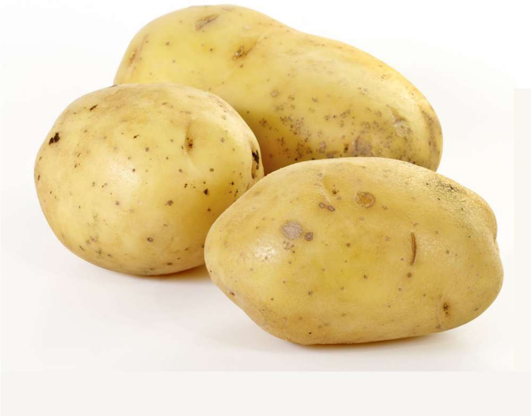
Recent trend: exhaustive search in $\sqrt{N}$

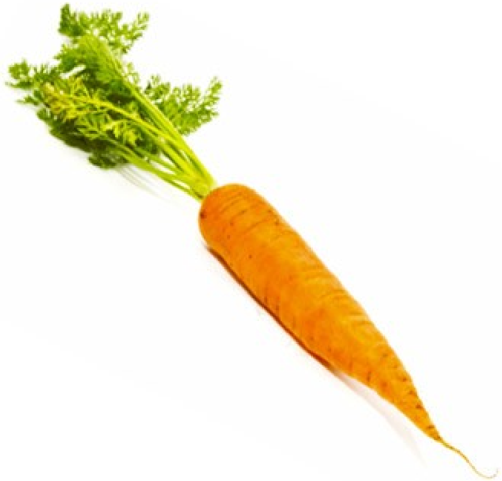
Primitive roots

$$\boldsymbol{\alpha} \in \mathbb{F}_{2^n}$$

Primitive roots

$$\alpha \in \mathbb{F}_{2^n}$$



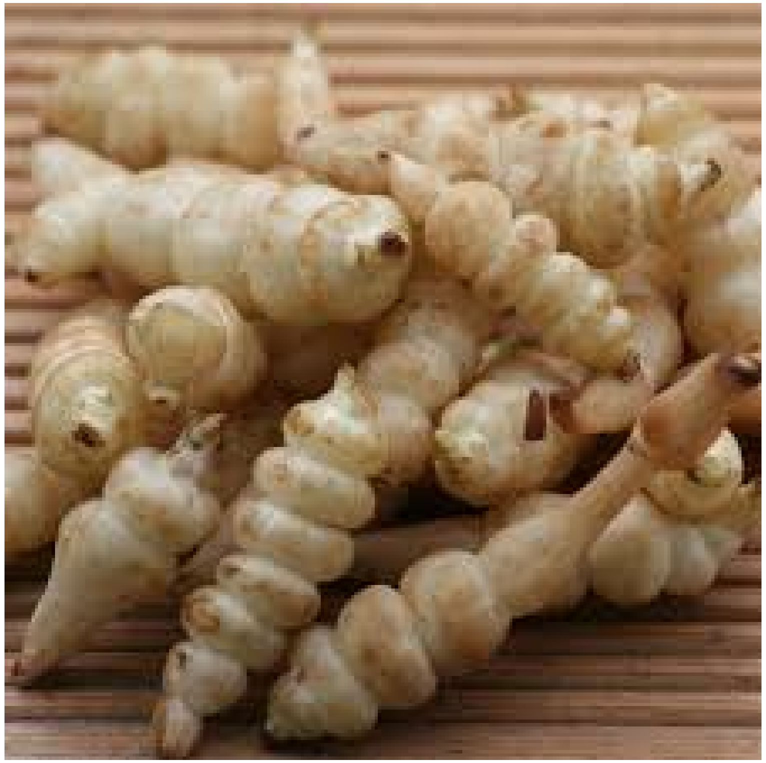


More complex roots

$$\exp\left(\frac{2\pi i}{n}\right)$$

Very complex roots

Chinese artichokes



Many thanks to Jérémy JEAN

Many thanks to Jérémy JEAN

Many thanks to Florian MENDEL and Yu SASAKI

Remaining open problem

To beet or not to beet: that is the question.