Computing finite fields' embeddings

Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean-Pierre Flori, Éric Schost

ANSSI, UVSQ, University of Western Ontario

September 28, 2015

Computing fi[illegible] embeddings

USING CATS

Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean-Pierre Flori, Éric Schost

ANSSI, UVSQ, University of We[illegible]

September 28, 2[illegible]

Random (keyboard) cat

$$\begin{array}{ccc} \mathsf{F}_{q^r} & \subseteq & \mathsf{F}_q[X]/(f(X)) \\ \downarrow & & \uparrow \\ \mathsf{F}_{q^r} & \subseteq & \mathsf{F}_q[X]/(g(X)) \end{array}$$

Random (keyboard) cat

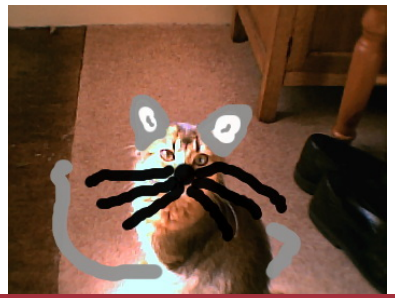
$$\begin{array}{ccc} \mathsf{F}_{q^r} & \subseteq & \mathsf{F}_q[X]/(f(X)) \\ \downarrow & & \downarrow \\ \mathsf{F}_{q^r} & \subseteq & \mathsf{F}_q[X]/(g(X)) \end{array}$$

Different minimal polynomials . . .

Cycl(otom)ic cat

Fix a minimal polynomial
with easy to compute roots

$$x^l = 1$$

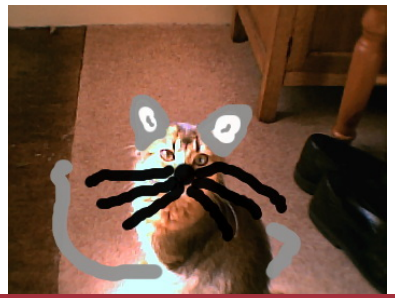


Cycl(otom)ic cat

Fix a minimal polynomial with easy to compute roots

$$x^l = 1$$

Cats are not Galois conjugates!



Gauss period cats

Sum the cats!

$$< q_r, H >= \mathsf{F}_l^{\times}, \sum_{h \in H} x^h$$

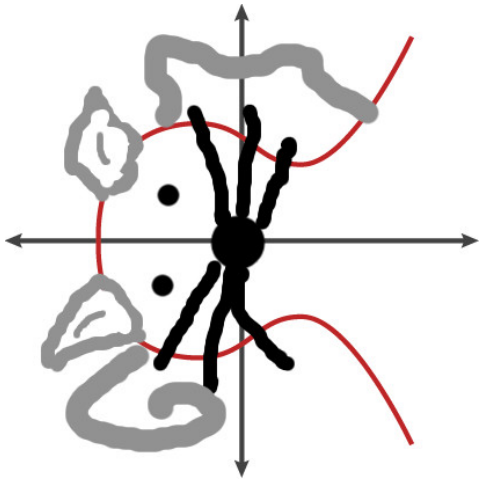
Gauss period cats

(Use Gauss periods)

Sum the cats!

$$< q_r, H >= \mathsf{F}_l^{\times}, \sum_{h \in H} x^h$$

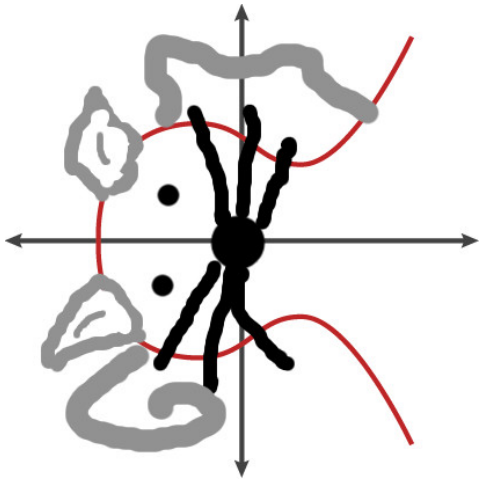
Elliptic period cats



What about elliptic period cat?

$< \lambda_r, H >= \mathsf{F}_l^{\times}/\{\pm 1\}, \sum_{h \in H}([h]P_r)_x$

Elliptic period cats



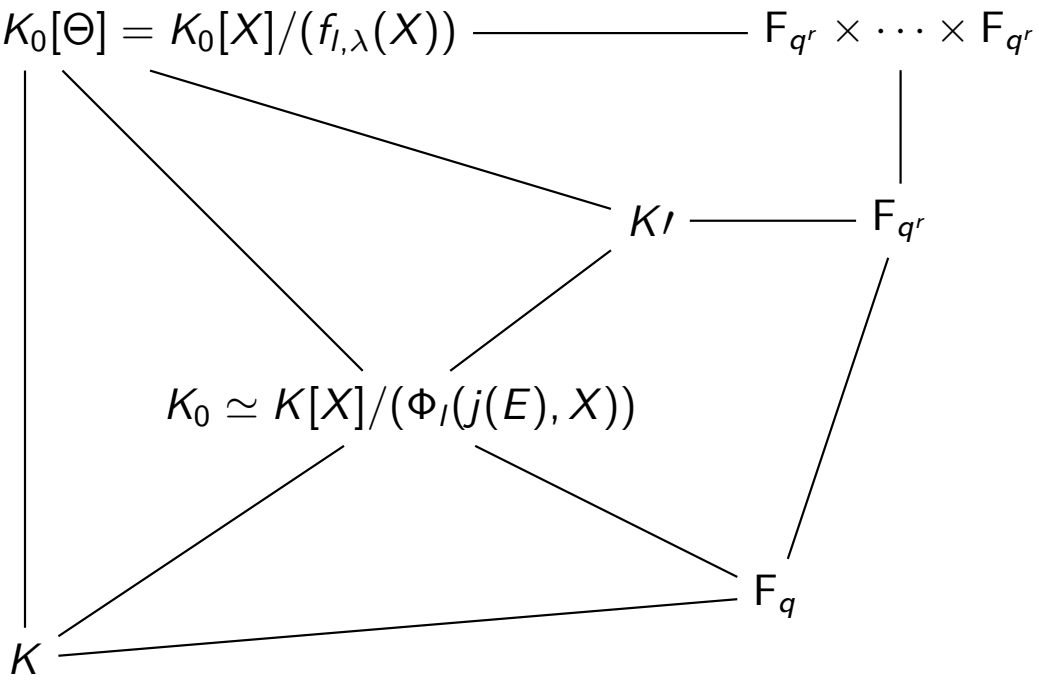
What about elliptic period cat?

$< \lambda_r, H >= \mathsf{F}_l^{\times}/\{\pm 1\}, \sum_{h \in H}([h]P_r)_x$

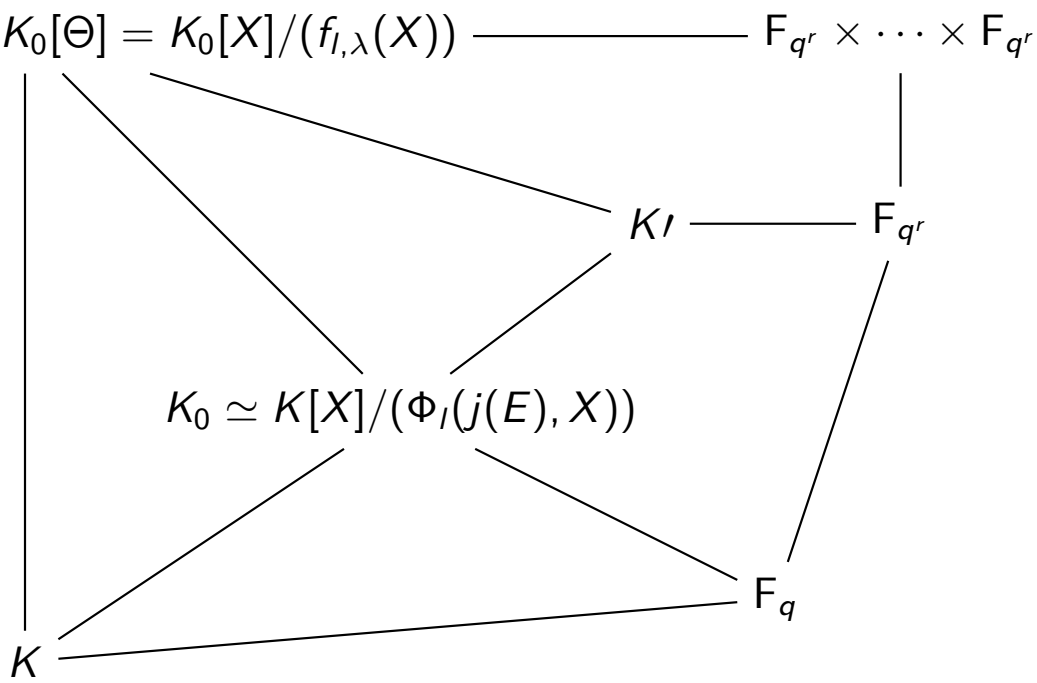
(Mentioned in MMS)

Works well in practice, but no proof so far

The (rainbow) diagram



The (rainbow) diagram



Suggestions welcome!!!

Other cat species

Github repository

More fun at

`https://github.com/defeo/ffisom/`