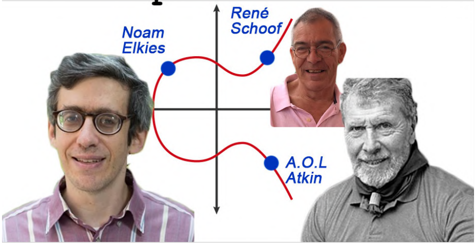
Towards generalization of SEA to hyperelliptic curves

Nikita Kolesnikov
PhD Student
Immanuel Kant Baltic Federal University

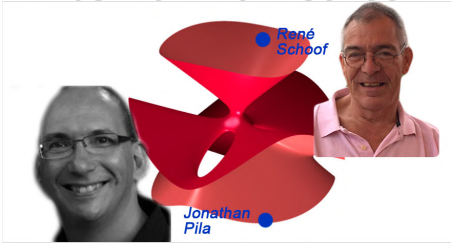
ECC 2019, rump session

December 02, 2019

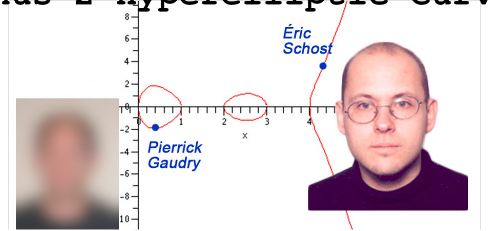
Elliptic Curves



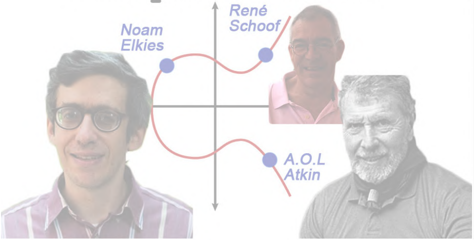
Abelian Varieties



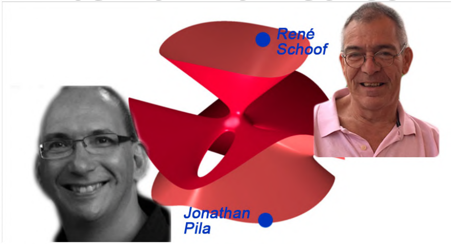
Genus 2 Hyperelliptic Curves



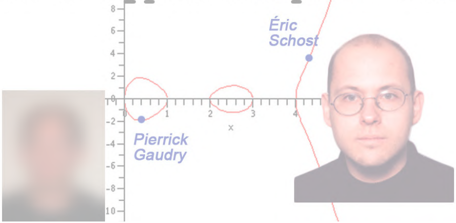
Elliptic Curves



Abelian Varieties



Genus 2 Hyperelliptic Curves



Motivation

- Let A be an abelian surface over $\mathbb{F}_q$, $char(\mathbb{F}_q) = p$
- $A \sim E_1 \times E_2$ or $A \sim J_C$
- Fix some ℓ prime and consider ℓ-torsion subgroup $A[\ell]$
- Calculate the order $\text{ord}(Frob_{A[\ell]})$ of Frobenius action on $A[l]$.

How to calculate this?

Motivation

- Let A be an abelian surface over $\mathbb{F}_q$, $char(\mathbb{F}_q) = p$
- $A \sim E_1 \times E_2$ or $A \sim J_C$
- Fix some ℓ prime and consider ℓ-torsion subgroup $A[\ell]$
- Calculate the order $\mathrm{ord}(Frob_{A[\ell]})$ of Frobenius action on $A[l]$.

How to calculate this?

Motivation

- Let A be an abelian surface over $\mathbb{F}_q$, $char(\mathbb{F}_q) = p$
- $A \sim E_1 \times E_2$ or $A \sim J_C$
- Fix some ℓ prime and consider ℓ-torsion subgroup $A[\ell]$
- Calculate the order $\mathrm{ord}(Frob_{A[\ell]})$ of Frobenius action on $A[l]$.

How to calculate this?

Motivation

- Let A be an abelian surface over $\mathbb{F}_q$, $char(\mathbb{F}_q) = p$
- $A \sim E_1 \times E_2$ or $A \sim J_C$
- Fix some ℓ prime and consider ℓ-torsion subgroup $A[\ell]$
- Calculate the order $\text{ord}(Frob_{A[\ell]})$ of Frobenius action on $A[l]$.

How to calculate this?

Orders of matrices in $Sp_4(\mathbb{F}_\ell)$

Classes in $Sp_4(\mathbb{F}_\ell)$	Order of matrices (projective)	Probability $(M \in Sp_4(\mathbb{F}_\ell) \wedge M \in class)$
$\overline{A_1}, \overline{A_1'}$	1	$1/(\ell^4(\ell^2-1)(\ell^4-1))$
$\overline{B_1(i)}$	$\frac{\ell^2+1}{2s}$, $s = \gcd(i, \frac{\ell^2+1}{2})$	$1/(\ell^2+1)$
$\overline{B_2(i)}$	$\frac{\ell^2-1}{2s}$, $s = \gcd(i, \frac{\ell^2-1}{2})$	$1/(\ell^2-1)$
$\overline{B_3(i,j)}$	$\frac{\ell-1}{\gcd(\ell-1, i+j, \lvert i-j \rvert)}$	$1/(\ell-1)^2$
$\overline{B_4(i,j)}$	$\frac{\ell+1}{\gcd(\ell+1, i+j, \lvert i-j \rvert)}$	$1/(\ell+1)^2$
$\overline{B_5(i,j)}$	$\frac{\ell^2-1}{\gcd(\ell^2-1, i(\ell-1)+j(\ell+1), 2i(\ell-1))}$	$1/(\ell^2-1)$
$\overline{B_6(i)}$	$\frac{\ell+1}{2s}$, $s = \gcd(i, \frac{\ell+1}{2})$	$1/(\ell(\ell+1)(\ell^2-1))$
$\overline{B_7(i)}$	$\frac{\ell(\ell+1)}{2s}$, $s = \gcd(i, \frac{\ell(\ell+1)}{2})$	$1/(\ell(\ell+1))$
$\overline{B_8(i)}$	$\frac{\ell-1}{2s}$, $s = \gcd(i, \frac{\ell-1}{2})$	$1/(\ell(\ell-1)(\ell^2-1))$
$\overline{B_9(i)}$	$\frac{\ell(\ell-1)}{2s}$, $s = \gcd(i, \frac{\ell(\ell-1)}{2})$	$1/(\ell(\ell-1))$

The distribution of orders

ord	$(1,\ell]$	$(\ell,2\ell]$	$\frac{\ell^2-1}{2}$	$\frac{\ell^2+1}{2}$	$\frac{\ell^2-1}{4}$	$\frac{\ell^2+1}{4}$	*Other*
Prob	0.193	0.065	0.134	0.157	0.066	0.050	0.335

- Result:
  - the orders $\mathrm{ord}(Frob_{A[\ell]})$ are sorted by probabilities.
- Further work:
  - Apply the distribution of orders to point counting algorithm.
- Any insight in this direction will be appreciated.

https://crypto-kantiana.com/nikita.kolesnikov/
NiKolesnikov@kantiana.ru

Thank you!