Affine algebraic geometry and a symmetric key application

Stefan Maubach

December 2011

How this talk is organised:

- What cryptographic/security problem will I work towards?
- Affine algebraic geometry
- Polynomial maps over $\mathbb{F}_q$: theoretically interesting things
- Polynomial maps over $\mathbb{F}_q$: cryptographic aspects

Symmetric key-key

	Alice	TheWorld	Bob
Secretkey	K		K
Message	M		
Encryption		$\xrightarrow{E_K(M)}$	
Decryption			$D_K(E_K(M))$

Session-keys

	Alice	*TheWorld*	*Bob*
Secret key	K		K
$*Protocol*$			
Session key	S		S
Message	M		
Encryption		$\xrightarrow{E_S(M)}$	
Decryption			$D_S(E_S(M))$

Session-keys: Diffie-Hellmann protocol

	Alice	*TheWorld*	*Bob*
Secret key	$K(x)$		$K(x)$
Known formula		$f(x,y)$	
Random value	a		b
Send :		$\xrightarrow{f(K,a)}$	
		$\xleftarrow{f(K,b)}$	
Compute	$f(f(K,b),a)$		$f(f(K,a),b)$
Session key	$S :=$		$S :=$

- $f(f(x,y),z) = f(f(x,z),y)$
- $f(x,y)$ gives no info on x if y is random

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{ccl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{ccl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Geometrically sometimes "more difficult" than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Geometrically sometimes "more difficult" than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

Subtopic - but of *fundamental importance* to the whole of Algebraic geometry.

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$
\begin{array}{ccl}
k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\
V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V)
\end{array}
$$

Geometrically sometimes "more difficult" than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

Subtopic - but of *fundamental importance* to the whole of Algebraic geometry.

We do all kinds of advanced things with algebraic geometry, but still we don't understand affine n-space k^n !

A Very Brief History

"Originally": geometry and algebra different things.

Zariski $\longrightarrow$ Grothendieck $\longrightarrow$ etc.: **algebraic geometry**.

$+$- 1970: What if we apply algebraic geometry to the original simple objects, like $\mathbb{C}^n$, or $\mathbb{C}[X_1, X_2, \ldots, X_n]$?

("Birth" of the field and many of its current questions.)

Since then: steady growth of the field.

(2000: separate AMS classification.)

$$\begin{aligned} k^n &\leftrightarrow k[X_1, \ldots, X_n] \\ V &\leftrightarrow \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{aligned}$$

Objects, hence morphisms!

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Objects, hence morphisms!

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

$$
\begin{array}{rcl}
k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\
V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V)
\end{array}
$$

Objects, hence morphisms!

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

Set of polynomial automorphisms of k^n:

$Aut_n(k)$, also denoted by $\mathrm{GA}_n(k)$ - similarly to $\mathrm{GL}_n(k)$!

A topic is defined by its problems.

Many problems in AAG: inspired by linear algebra!
(In some sense: AAG most "natural generalization of linear algebra"...)
Will show two problems: (1) Jacobian Conjecture, (2) generators problem

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$L \in \mathrm{GL}_n(k)$ invertible $\iff$ $\det(L) = \det(\mathrm{Jac}(L)) \in k^*$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rccl} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$G \circ F = (X_1, \ldots, X_n).$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\mathrm{Jac}(G \circ F) = \mathrm{Jac}(X_1, \ldots, X_n).$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\mathrm{Jac}(G \circ F) = I.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{lccc} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F) = I.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \cdot \det(\mathrm{Jac}(G) \circ F) = \det I = 1.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \cdot \det(blabla) = \det I = 1.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rccr} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \in k[X_1, \ldots, X_n]^* = k^*.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$
\begin{array}{rcll}
L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\
F \in \mathrm{GA}_n(k) \text{ invertible} & \Longrightarrow & & \det(\mathrm{Jac}(F)) \in k^*
\end{array}
$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \in k[X_1, \ldots, X_n]^* = k^*.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Longrightarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

Jacobian Conjecture:

$$F \in \mathrm{GA}_n(k) \mathit{invertible} \Longleftarrow \det(\mathrm{Jac}(F)) \in k^*$$

"Visual" version of Jacobian Conjecture

Volume-preserving polynomial maps are invertible.

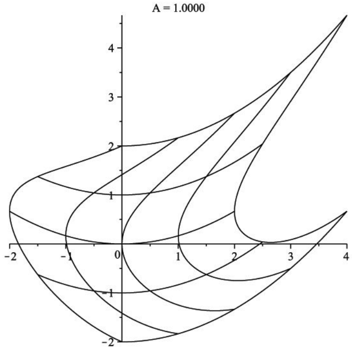

Figure: Image of raster under $(X + \frac{1}{2}Y^2, Y + \frac{1}{6}(X + \frac{1}{2}Y^2)^2)$.

Jacobian Conjecture very particular for *polynomials:*

$$F : (x, y) \longrightarrow (e^x, ye^{-x})$$

$$\mathrm{Jac}(F) = \begin{pmatrix} e^x & 0 \\ -ye^{-x} & e^{-x} \end{pmatrix}$$

$$\det(\mathrm{Jac}(F)) = 1$$

Jacobian Conjecture in $\mathrm{char}(k) = p$:

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \iff & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

Jacobian Conjecture in $\mathrm{char}(k) = p$:

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

$$\begin{aligned} F: \quad k^1 &\longrightarrow k^1 \\ X &\longrightarrow X - X^p \end{aligned}$$

$Jac(F) = 1$ but $F(0) = F(1) = 0$.

Jacobian Conjecture in $\mathrm{char}(k) = p$:

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

$$\begin{aligned} F: \quad k^1 &\longrightarrow k^1 \\ X &\longrightarrow X - X^p \end{aligned}$$

$Jac(F) = 1$ but $F(0) = F(1) = 0$.

Jacobian Conjecture in char$(k) = p$**:** Suppose $\det(Jac(F)) = 1$ and $p \nmid [k(X_1, \dots, X_n) : k(F_1, \dots, F_n)]$. Then F is an automorphism.

Jacobian Conjecture in $\mathrm{char}(k) = p$:

$\mathrm{char}(k) = 0$:

$F = (X + a_1X^2 + a_2XY + a_3Y^2, Y + b_1X^2 + b_2XY + b_3Y^2)$

$$\begin{aligned} 1 = \; & \det(Jac(F)) \\ = \; & 1+ \\ & (2a_1 + b_2)X+ \\ & (a_2 + 2b_3)Y+ \\ & (2a_1b_2 + 2a_2b_1)X^2+ \\ & (2b_2a_2 + 4a_1b_3 + 4a_3b_1)XY+ \\ & (2a_2b_3 + 2a_3b_2)Y^2 \end{aligned}$$

In char(k)=2 : (parts of) equations vanish. **Question:** What are the right equations in $\mathrm{char}(k) = 2$? (or p?)

Enough about the Jacobian Problem! Another problem:

Generator problem

Understanding polynomial automorphisms

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \dots, X_n), \dots, F_n(X_1, \dots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.
- A ring automorphism of $k[X_1, \ldots, X_n]$ sending $g(X_1, \ldots, X_n)$ to $g(F_1, \ldots, F_n)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) = & \ ([X - Y^2] + [Y]^2, [Y]) \\ = & \ (X - Y^2 + Y^2, Y) \\ = & \ (X, Y).\end{aligned}$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!

Understanding polynomial automorphisms

Remark: If k is algebraically closed, then a polynomial endomorphism $k^n \longrightarrow k^n$ which is a bijection, is an invertible polynomial map.

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

$GA_n(k)$ is generated by ???

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

$TA_n(k) :=< J_n(k), Aff_n(k) >$

In dimension 1: we understand the automorphism group.

(They are linear.)

In dimension 1: we understand the automorphism group. (They are linear.)
In dimension 2: famous Jung-van der Kulk-theorem:

$$\mathrm{GA}_2(\mathbb{K}) = \mathrm{TA}_2(\mathbb{K}) = \mathit{Aff}_2(\mathbb{K}) \ltimes \mathrm{J}_2(\mathbb{K})$$

Jung-van der Kulk is the reason that we can do a lot in dimension 2 !

What about dimension 3?

What about dimension 3? Stupid idea: everything will be tame?

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: “I cannot tame the following map:”

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata’s map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

(Difficult and technical proof.) (2007 AMS Moore paper award.)

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!! ...in characteristic ZERO...

(Difficult and technical proof.) (2007 AMS Moore paper award.)

AMS E.H. Moore Research Article Prize

 Ivan Shestakov (center) and Ualbai Umirbaev (right) with Jim Arthur.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map

$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{Bij}_n(\mathbb{F}_q)$.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?
Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map
$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{Bij}_n(\mathbb{F}_q)$.
What is $\pi_q(\mathrm{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map

$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{Bij}_n(\mathbb{F}_q)$.

What is $\pi_q(\mathrm{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

Simpler question: what is $\pi_q(\mathrm{TA}_n(\mathbb{F}_q))$?

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$? (open since 2000).

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$?

(open since 2000). So, if $\pi_4(N) \notin \mathsf{Alt}$, then N is not tame!

$\longrightarrow$ 1-page paper in Inventiones Mathematicae !

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$? (open since 2000). So, if $\pi_4(N) \notin \mathsf{Alt}$, then N is not tame! $\longrightarrow$ 1-page paper in Inventiones Mathematicae ! So, let's check:

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$? (open since 2000). So, if $\pi_4(N) \notin \mathsf{Alt}$, then N is not tame! $\longrightarrow$ 1-page paper in Inventiones Mathematicae ! So, let's check: ...dromroll...

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$? (open since 2000). So, if $\pi_4(N) \notin \mathsf{Alt}$, then N is not tame! $\longrightarrow$ 1-page paper in Inventiones Mathematicae ! So, let's check: ...dromroll... how sad, $\pi_4(N)$ even.

Theorem:

If q is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

Obvious question: $\pi_4(\mathsf{TA}_n(\mathbb{F}_4)) = \mathsf{Alt}(4^n)$ or $\mathsf{Sym}(4^n)$?
(open since 2000). So, if $\pi_4(N) \notin \mathsf{Alt}$, then N is not tame!
$\longrightarrow$ 1-page paper in Inventiones Mathematicae ! So, let's check: $\ldots$dromroll$\ldots$ how sad, $\pi_4(N)$ even.
Also, $\pi_q(N)$ even if and only if $q = 2^m, m \geq 2\ldots$bummer!

Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

Example: $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

Example: $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

Lemma: $p(x) \sim q(x)$ in $k[x, y_1, \ldots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

Example: $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

Lemma: $p(x) \sim q(x)$ in $k[x, y_1, \ldots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

If *chark* $= 0$, this implies $p(x) \sim q(x)$ in $k[x]$.

Equivalence of polynomials

Let $p, q \in k[x_1, \dots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \dots, x_n)\tau = (q, x_2, \dots, x_n)$.

Example: $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

Lemma: $p(x) \sim q(x)$ in $k[x, y_1, \dots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

If $char k = 0$, this implies $p(x) \sim q(x)$ in $k[x]$.

If $char k = p \dots$

Are $x^8 + x^4 + x$ and $x^8 + x^2 + x$ equivalent in $\mathbb{F}_2[x, y, z]$?

Mock automorphisms

$F \in MA_n(\mathbb{F}_q)$ is called a *mock automorphism* if

- $\det(Jac(F)) \in \mathbb{F}_q^*$
- $\pi_q(F)$ is a bijection

$x^8 + x^4 + x$ and $x^8 + x^2 + x$ are mock automorphisms for $\mathbb{F}_{2^m}$ if $7 \not| m$.

Equivalence classes of Mock automorphisms

Theorem: If $F \in MA_3(\mathbb{F}_2)$ of degree ≤ 2, then F is equivalent to:

Equivalence classes of Mock automorphisms

Theorem: If $F \in MA_3(\mathbb{F}_2)$ of degree ≤ 2, then F is equivalent to:

- (x, y, z)

Equivalence classes of Mock automorphisms

Theorem: If $F \in MA_3(\mathbb{F}_2)$ of degree ≤ 2, then F is equivalent to:

- (x, y, z)
- $(x^4 + x^2 + x, y, z)$

Equivalence classes of Mock automorphisms

Theorem: If $F \in MA_3(\mathbb{F}_2)$ of degree ≤ 2, then F is equivalent to:

- (x, y, z)
- $(x^4 + x^2 + x, y, z)$
- $(x^8 + x^2 + x, y, z)$
- $(x^8 + x^4 + x, y, z)$

Equivalence classes of Mock automorphisms

Theorem: If $F \in MA_3(\mathbb{F}_2)$ of degree ≤ 2, then F is equivalent to:

- (x, y, z)
- $(x^4 + x^2 + x, y, z)$
- $(x^8 + x^2 + x, y, z)$
- $(x^8 + x^4 + x, y, z)$

…but are there 3 or 4 equivalence classes?

Degree 3 over $\mathbb{F}_2$

	Representant	Bijection over	#
1.	(x, y, z)	all	400
2.	$(x, y, z + x^3z^4 + xz^2)$	$\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}, \mathbb{F}_{32}$	56
3.	$(x, y, z + x^3z^2 + x^3z^4)$	$\mathbb{F}_2, \mathbb{F}_4$	168
4.	$(x, y, z + xz^2 + xz^6)$	$\mathbb{F}_2$	336
5.	$(x, y, z + x^3z^2 + xy^2z^4 + x^2yz^4 + x^3z^6)$	$\mathbb{F}_2$	336
6.	$(x, y, z + x^3z^2 + xy^2z^2 + x^2yz^4 + x^3z^6)$	$\mathbb{F}_2$	168
7.	$(x + y^2z, y + x^2z + y^2z, z + x^3 + xy^2 + y^3)$	$\mathbb{F}_2$	56

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM…)

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Public key.

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

(complicated map) $\longleftarrow$ Public key.

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(complicated map) $\longleftarrow$ Public key.

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(elementary) $\times$ (affine) $\times$ (elementary) $\times \ldots \times$ (elementary)

$=$ (complicated map) $\longleftarrow$ Public key.

Public key crypto

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(elementary) $\times$ (affine) $\times$ (elementary) $\times \ldots \times$ (elementary)

$=$ (complicated map) $\longleftarrow$ Public key.

Nice idea - basic idea still uncracked, but: a lot of attacks on implementations (Goubin, Courtois, etc.)

Additive group actions

Characteristic 0: $(k, +)$-action on k^n

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Additive group actions

Characteristic 0: $(k,+)$-action on k^n

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

$$(1 \times (x, y, z) \longrightarrow (x + y + z, y + z, z))$$

Additive group actions

Characteristic 0: $(k, +)$-action on k^n

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

$$(1 \times (x, y, z) \longrightarrow (x + y + z, y + z, z))$$

Is the same as:

$$t \times (x, y, z) \longrightarrow (\exp(tD)(x), \exp(tD)(y), \exp(tD)(z))$$

where

$$D := (y + \frac{1}{2} z) \frac{\partial}{\partial x} + z \frac{\partial}{\partial y}.$$

(a *locally nilpotent derivation*)

Additive group actions

Characteristic p: $(k,+)$-action on k^n

Example:

$$t \times (x,y,z) \longrightarrow (F_1(t,x,y,z), F_2(t,x,y,z), F_3(t,x,y,z))$$

Is the same as:

$$t \times (x,y,z) \longrightarrow (\exp(tD)(x), \exp(tD)(y), \exp(tD)(z))$$

where

$$D$$

(is a *locally finite iterative higher derivation*)

Additive group actions char. p: problems

Characteristic 2: $(k,+)$-action on k^n

Example:

$$t \times (x,y,z) \longrightarrow (x + ty + \frac{t^2+t}{2} z, y + tz, z)$$

is NOT a $(k,+)$ action! In particular,

$$(x+y+z, y+z, z)$$

is not the exponent of a locally finite iterative higher derivation. Any k-action has order p !

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

Theorem: If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Corollary: If $f(x) \in \mathbb{Q}[x]$ such that $f \mod p$ makes sense, then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

Additive group actions char. p: solution

Char$= 0$: $(x + ty + \frac{t^2+t}{2}z, y + tz, z) \in k[t][x, y, z]$

Additive group actions char. p: solution

Char$=0$: $\left(x+ty+\frac{t^2+t}{2}z, y+tz, z\right) \in k[t][x,y,z]$

Char$=2$: $\left(x+ty+(Q_1+t)z, y+tz, z\right) \in k[t,Q_1][x,y,z]$

where $Q_1 := \binom{t}{2}$.

Additive group actions char. p: solution

Char$=0$: $(x + ty + \frac{t^2+t}{2}z, y + tz, z) \in k[t][x, y, z]$
Char$=2$: $(x + ty + (Q_1 + t)z, y + tz, z) \in k[t, Q_1][x, y, z]$
where $Q_1 := \binom{t}{2}$.
In general:

$$R := k[Q_i; i \in \mathbb{N}] \text{ where } Q_i := \binom{t}{p^i}.$$

$$F \in GA_n(R)$$

Strictly upper triangular group

$$B_n(k) := \{(x_1 + f_1, \ldots, x_n + f_n \; ; \; f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

Strictly upper triangular group

$$B_n(k) := \{(x_1 + f_1, \ldots, x_n + f_n \; ; \; f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n\ ;\ f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$$

Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n \, ; \, f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$

$\mathcal{B}_n(\mathbb{F}_p)$ is p-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$!

Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1,\ldots,x_n+f_n\,;\ f_i \in k[x_{i+1},\ldots,x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$

$\mathcal{B}_n(\mathbb{F}_p)$ is p-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$!

$$(x_1+f_1,\ldots,x_n+f_n) \in \mathcal{B}_n(\mathbb{F}_p)$$

$$f_i \in k[x_{i+1},\ldots,x_n]/(x_{i+1}^p - x_{i+1},\ldots,x_n^p - x_n)$$

Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n\ ;\ f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$

$\mathcal{B}_n(\mathbb{F}_p)$ is p-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$!

$$(x_1 + f_1, \ldots, x_n + f_n) \in \mathcal{B}_n(\mathbb{F}_p)$$

$$f_i \in k[x_{i+1}, \ldots, x_n]/(x_{i+1}^p - x_{i+1}, \ldots, x_n^p - x_n)$$

(*)

Session-keys: Diffie-Hellmann protocol

	$Alice$	$TheWorld$	Bob
$Secret\ key$	$K(x)$		$K(x)$
$Known\ formula$		$f(x,y)$	
$Random\ value$	a		b
$Send:$		$\xrightarrow{f(K,a)}$	
		$\xleftarrow{f(K,b)}$	
$Compute$	$f(f(K,b),a)$		$f(f(K,a),b)$
$Session\ key$	$S :=$		$S :=$

- $f(f(x,y),z) = f(f(x,z),y)$
- $f(x,y)$ gives no info on x if y is random

Session-keys: Diffie-Hellmann protocol

	Alice	*TheWorld*	*Bob*
Secret key	$\sigma(x)$		$\sigma(x)$
Known formula		$\sigma^y(x)$	
Random value	a		b
Send :		$\xrightarrow{\sigma^a(0)}$	
		$\xleftarrow{\sigma^b(0)}$	
Compute	$\sigma^a\sigma^b(0)$		$\sigma^b\sigma^a(0)$
Session key	$S :=$		$S :=$

- $f(f(x,y),z) = f(f(x,z),y)$
- $\sigma^a(0)$ gives no info on σ if a is random

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- Knowing several session keys gives no/little information on guessing the next session key hearing $\sigma^b(0), \sigma^a(0)$,
- To compute $\sigma^a(v)$ easily for any $a \in \mathbb{N}, v \in \mathbb{F}_p^n$.

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- Knowing several session keys gives no/little information on guessing the next session key hearing $\sigma^b(0), \sigma^a(0)$,
- To compute $\sigma^a(v)$ easily for any $a \in \mathbb{N}, v \in \mathbb{F}_p^n$.

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So,

$\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.

$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So,
$\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.
$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch. By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$. $\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

To prove: $\sum_{i=1}^{p^{n-1}} f(\tilde{\sigma}^i \alpha) = 0$ if and only if coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_1 is nonzero.

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch.

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Maps having one orbit only

Theorem 1.

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of f_i is nonzero.

Proofsketch.

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

Lemma

Let $M(x_1, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ *where* $0 \leq a_i \leq p-1$ *for each* $1 \leq i \leq n$. *Then* $\sum_{\alpha \in \mathbb{F}_p^n} M(\alpha) = 0$ *unless* $a_1 = a_2 = \ldots = a_n = p - 1$, *when it is* $(-1)^n$.

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- Knowing several session keys gives no/little help on guessing the next session key hearing $\sigma^a(0), \sigma^b(0)$.
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

Some degree of forward security

Situation: cracking m session keys means: adversary knows m triples $\sigma^{a_i}(0), \sigma^{b_i}(0), \sigma^{a_i+b_i}(0)$

Some degree of forward security

Situation: cracking m session keys means: adversary knows m triples $\sigma^{a_i}(0), \sigma^{b_i}(0), \sigma^{a_i+b_i}(0)$

Claim: less or equal to giving m pairs $(\sigma(v_i), v_i)$ where v_i is random.

Some degree of forward security

Situation: cracking m session keys means: adversary knows m triples $\sigma^{a_i}(0), \sigma^{b_i}(0), \sigma^{a_i+b_i}(0)$

Claim: less or equal to giving m pairs $(\sigma(v_i), v_i)$ where v_i is random.

Now we can prove: If there are $\log_p(m)$ pairs $(\sigma(v_i), v_i)$ known, then the last $[\log_p(m)]$ coordinates of a new key are computable, and the first $n - [\log_p(m)]$ no information is given on.

Some degree of forward security

Situation: cracking m session keys means: adversary knows m triples $\sigma^{a_i}(0), \sigma^{b_i}(0), \sigma^{a_i+b_i}(0)$

Claim: less or equal to giving m pairs $(\sigma(v_i), v_i)$ where v_i is random.

Now we can prove: If there are $\log_p(m)$ pairs $(\sigma(v_i), v_i)$ known, then the last $[\log_p(m)]$ coordinates of a new key are computable, and the first $n - [\log_p(m)]$ no information is given on.

$\longrightarrow$ don't use σ, but use $\varphi^{-1}\sigma\varphi$ where φ is some easily computable permutation!

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- Knowing several session keys gives no/little help on guessing the next session key hearing $\sigma^a(0), \sigma^b(0)$.
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Proof is very elegant but too long to elaborate on in this talk.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

Theorem 2. Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Theorem 3. After that, conjugating by a diagonal linear map $D \in \mathrm{GL}_n(\mathbb{F}_p)$ one can get all of them equivalent!

Hence, any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ having only one orbit can be written as

$$D^{-1}\tau^{-1}\Delta\tau D$$

where $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, D linear diagonal, and Δ is one particular map you choose in $\mathcal{B}_n(\mathbb{F}_p)$.

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be defined as

$$\zeta(a_1, a_2, \ldots, a_n) \longrightarrow a_1 + pa_2 + \ldots + p^{n-1}a_n$$

What is an easy map Δ?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then Δ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be defined as

$$\zeta(a_1, a_2, \ldots, a_n) \longrightarrow a_1 + pa_2 + \ldots + p^{n-1}a_n$$

Then

$$\zeta\Delta\zeta^{-1}(a) = a + 1, a \in \mathbb{Z}/p^n\mathbb{Z}$$

i.e. Δ^m is easy to compute! $\longrightarrow$ Cryptographic application is happy!

Just one more slide/ conclusions:

Just one more slide/ conclusions:

Polynomial maps over finite fields show promise in cryptographic applications - they are very natural permutation maps.

Just one more slide/ conclusions:

Polynomial maps over finite fields show promise in cryptographic applications - they are very natural permutation maps.

THANK YOU

(for enduring 142 .pdf slides...)