Registration form (basic details)

1a. Details of applicant

Title: dr.

First name: Stefan

Initials: S.J.

Prefix: none

Surname: Maubach

Gender: male

Work address (Address for correspondence):
Jacobs University
Campus Ring 1
28759 Bremen, Germany

Home Address:
An der Aue 62
28757 Bremen, Germany

Preference for correspondence in English: no

Telephone (work): ++49-421-200-3183

Telephone (home): ++49-421-62670686

Fax (work) : ++49-421-200-3103

email:
s.maubach@jacobs-university.de,
stefan.maubach@gmail.com

Family status:
Married to Joyce Hossu
(Lily Maubach, 22-12-2008, and Kim Maubach, 19-3-2011)

Website: http://www.math.ru.nl/~maubach/

1b. Title of research proposal

Algebraic endomorphisms of affine spaces and their applications

1c. Summary of research proposal (229 words; max 300 words)

The binding topic of this proposal is called Affine Algebraic Geometry (AAG). This topic focuses on automorphisms of affine spaces like $\mathbb{C}^n$ and $(\mathbb{F}_q)^n$. In this proposal, analytical maps and (formal) power series are considered, but the main focus is on polynomial automorphisms.

Polynomial automorphisms are a basic and important, but not very well understood, object in algebra and geometry. Currently, there are only a few (but often spectacular) links with other fields in mathematics, and hardly any outside of mathematics. The chosen topics for this proposal serve several goals:

Strenghten existing links and build new links of AAG with
- other fields of mathematics,
- applications, i.e. find applications and problems outside of mathematics for which AAG can provide solutions, and provide them.

This is done by:

I. Investigating polynomial maps over finite fields. This opens up links with number theory and finite group theory, as well as influencing applications in computer science, in particular cryptography. Concrete cryptographic applications are studied as well. (Topic I & V.)

II. Investigating locally finite polynomial and analytic automorphisms (opening up links with complex analysis and dynamical systems). Locally finite polynomial endomorphisms are maps which satisfy a recurrence relation. (Topic II)

III. Investigating Poisson algebras from a commutative agebra viewpoint (providing a different angle to an often studied object of mathematical physics), and studying modern invariants like the Makar-Limanov invariant. (Topic III & IV)

1d. Keywords

Affine algebraic geometry, Polynomial map, finite fields, locally finite map, cryptography.

1e. Host institution

Eindhoven University of Technology

1f. NWO Division

Exacte Wetenschappen (EW)

1g. NWO divisional discipline

In case you submit to one of the following divisions: *Physical sciences (EW), Humanities (GW), or Social/Behavioural sciences (MaGW),* please indicate the main NWO divisional discipline code, applicable to your application. For a list of these codes, please follow the division link (see Notes). You can select only one main code. You can indicate a second (additional) discipline code in case your research is multi-disciplinary within the NWO division.

Division				
EW	**First discipline code (main code)**	**Description**	**Second discipline code (additional)**	**Description**
	3	Mathematics	6	Mathematics and Computer Science

1h. NWO Domain

Beta

Research proposal

2a. Scientific/Scholarly quality

Introduction and mathematical background

A general remark at the start: this is mainly a pure mathematics proposal and as such motivated by internal questions of mathematics proper. However, part of my research is on trying to link the field with applications and other parts of mathematics.

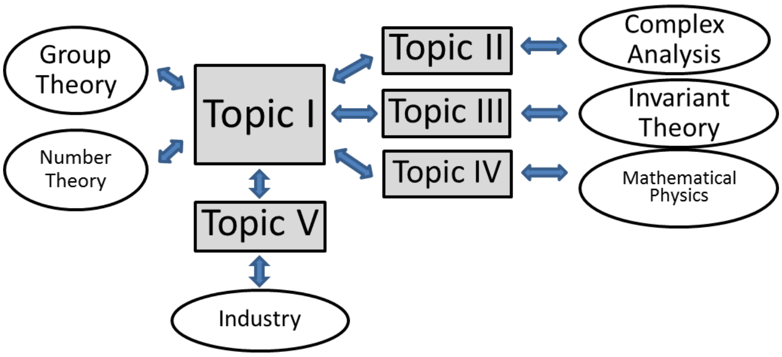
This section is meant to be a general outline, for non-experts having a mathematical background. The "Detailed Research Proposal" is more tailored towards experts, explaining in detail my research plans.

A recurring object in this proposal is that of a polynomial map F: $k^n \rightarrow k^n$ (k a field), which is called a polynomial automorphism if there exists a polynomial map G such that $F(G)=G(F)=(X_1,..,X_n)$. The simplest nonlinear example is $(X+ Y^2, Y)$, having inverse $(X-Y^2, Y)$.

What the linear automorphisms are for linear algebra, polynomial automorphisms are for (polynomial) algebras. As such, the set of polynomial automorphisms (or: algebraic automorphisms, or in this proposal: simply ``automorphisms'') is one of the most basic objects in algebra and algebraic geometry. Being a basic object does not mean understood, however: see for example the heading under ``The Generator Problem''. This proposal falls under the name of Affine Algebraic Geometry (abbreviated AAG in this proposal). This still growing topic has become its own research field since the late 1980's, and received its own AMS classification in 2000. A space like $\mathbb{C}^n$ (or k^n) is the simplest example of a so-called affine variety, and a very important one. In contrast to projective geometry and scheme-theoretic geometry, affine algebraic geometry is closer to algebra. There is a one-to-one correspondence between affine spaces (varieties) and zero-sets of polynomials, which in turn correspond to quotients of polynomial rings. Hence, in this field, it is very beneficial to switch back and forth between a geometric and algebraic viewpoint, making it a truly vibrant, interdisciplinary field.
Although AAG is the natural link between algebra and geometry, it does not yet live up to its full potential: so far its connections to other fields have been sporadic. But when they occur, they are often important and spectacular: some examples are the solution of the Markus-Yamabe conjecture [1] in dynamical systems, counterexamples to Hilbert's 14th problem [2] in invariant theory, or the recent contributions by Belov and Kontsevich [3] using Lie brackets, Possion and Weyl algebras, and reduction-mod-p-techniques *(This list of three cases is not comprehensive, but just a choice! A few others (again not comprehensive):[4,5].).* One of the underlying thoughts that I want to convey in this proposal is:
Polynomial automorphisms can be connected with more topics than they habitually are. This viewpoint influences my research a lot, which is reflected in the following subdivision of the proposal into subtopics, all evolving around the central theme of the polynomial automorphism group:
I. Number theory and finite groups: by investigating polynomial endomorphisms over finite fields.[40%]
II. Dynamical systems and complex analysis: by investigating locally finite polynomial endomorphisms.[15%]
III. Modern Invariants: geometric properties of the Makar-Limanov invariant and related invariants. [15%]
IV. Poisson algebras: by studying the automorphisms of commutative polynomial rings endowed with a Poisson bracket.[10%]

V. Cryptography: applying polynomial maps to symmetric key cryptography.[20%]

The connections could go both ways: applying polynomial maps to the other field, or vice versa, depending on the problem. Between brackets I put an indication of the expected relative size, which should not be understood very rigidly. In fact, the subjects overlap (for example, cryptography can be seen as a subtopic of the first one). First, I will state (the) three major problems related to my research, to give the reader the current state of affair.



Schematic diagram of connections between topics.

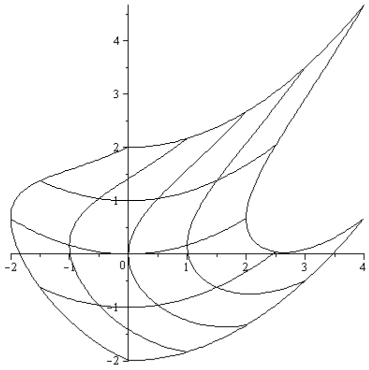
Notations and definitions: The polynomial automorphism group in dimension n over a ring R is denoted by $GA_n(R)$. The tame automorphism group in dimension n over a ring R is denoted by $TA_n(R)$. It is defined as the subgroup of automorphisms generated by linear automorphisms and triangular automorphisms $(X_1+f_1(X_2,\ldots,X_n), X_2+f_2(X_3,\ldots,X_n), \ldots, X_n+f_n)$. The letter k is used for a field, and $Bij(k^n)$ for the set of bijections of k^n.

The generator problem.
$GA_1(k)$ equals $GL_1(k)$, and is considered trivial. $GA_2(k)$ is known, due to the famous Jung-van der Kulk theorem, and among others states that $GA_2(k)=TA_2(k)$. This theorem is one of the reasons why many results are obtained in dimension 2. However, in dimension 3 and up, we don't even know if we have a set of generators for the automorphism group $GA_n(k)$! Many a problem on a group is completely unfeasible if one doesn't know generators of the group, and we severely suffer from this deficit here. In fact, the most celebrated recent progress in this direction is in essence a negative result by Umirbaev-Shestakov [6], which states that $GA_3(k)\neq TA_3(k)$. This inequality was conjectured already by Nagata in 1972, who discovered the now named Nagata-automorphism $N(X,Y,Z)=(X-2Y\Delta-Z\Delta^2, Y+Z\Delta, Z)$ where $\Delta=XZ+Y^2$. He conjectured that this automorphism was not tame, but it took more than 30 years to solve. Umirbaev-Shestakov were awarded the 2007 Moore AMS paper award for this feat. (Note that I will be working with Umirbaev intensively if supported by this proposal!) Together with a few other results like [7] it seems that finally we have significant progress. We are still far away from a true understanding, but *finally after 30 years* we have significant forward movement. In particular, it seems feasible to fully understand the subgroup $GA_2(k[X_3])$ of $GA_3(k)$, which fixes the last variable, a problem I am working on with excitement!

Classifying affine varieties. A basic problem is to determine if an affine variety V is isomorphic to another variety - and in particular, if $V \cong k^n$. A historically important 3-fold is the Koras-Russell threefold given by the equation $x^2y+x+z^2+t^3 = 0$.
It was proven by Makar-Limanov in [8] that this 3-fold was not isomorphic to k^3 by introducing what is now called the Makar-Limanov invariant. The interest in this invariant has been huge in the past few years. A related invariant is the Derksen invariant. The applicant proved in [9] that both invariants distinguish different varieties. A related problem is the Cancellation Conjecture, which states

that if V×k (the cylinder over V) is isomorphic to k^{n+1}, then V is isomorphic to k^n. This conjecture grew out of the general cancellation problem (which turned out to be false), asking if $V\times k \cong W\times k \rightarrow V \cong W$ holds. An important class of counterexamples to generalized cancellation are the Danielewski surfaces (like $x^n y+p(x,z) = 0$), but in [10] the applicant found the first UFD counterexamples, which was an important breakthrough towards attacking "the" Cancellation Problem. Recently, even contractible UFD counterexamples were found [11].

The Jacobian Conjecture. The most famous conjecture in AAG: it states that a polynomial endomorphism F for which the Jacobian determinant is a nonzero constant (i.e. det(Jac(F)) in k^*) must be an automorphism. (Another interesting way to state this, is to say that volume-preserving maps are invertible.) The problem is essentially a problem about polynomial *endomorphisms,* and as such has quite a different nature than the other problems mentioned here. In some sense, the only true progress on the problem in the last 30 years or so, is in finding many equivalent formulations. In the recent landmark paper [3] by Belov and Kontsevich it was proven that the Jacobian Conjecture is equivalent to the Dixmier Conjecture (which I won't explain here), linking two very important conjectures with each other. The main methods, also developed in later papers [12] , are transferring properties in characteristic p to characteristic zero, in connection with Weyl algebras and Poisson algebras. One of the main tools are reduction-mod-p-techniques: obtaining results over a field like the complex numbers, by first proving other results for finite fields. This result is also a source of inspiration for this proposal.



The image of a polynomial automorphism with Jacobian determinant one; each enclosed area equals 1.

Detailed Research Proposal

Below, I will describe my research proposal. From here on I go more in-depth, and as such some parts may be harder to read for non-experts. There are several linked sub-topics. In each topic I will point out a central question. The main point in each topic is not always to solve that question (completely), but to use it as a source of inspiration, or as a "name problem", representing a set of related interesting questions.

Topic I: Polynomial maps over finite fields

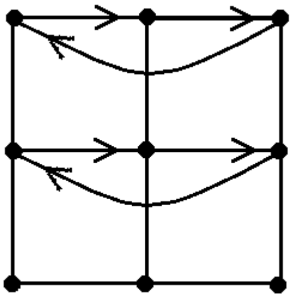
This subject forms the bulk of my proposal, the reason being its great potential and connection to applications (Topic V) and the fact that it is almost completely unexplored. At the moment it has already become a large part of my research. There is very little research on polynomial automorphisms specifically in characteristic p: if something is known in characteristic p, it is mostly because the result is true for characteristic zero and by a slight adaptation one proves it for any characteristic. However, for example in the result of Belov-Kontsevich, the use of characteristic p is all-important. When one restricts it even a little further to finite fields, it is shockingly void: there are literally only a handful of papers written on this topic, [13] one by me [14]. A sample question:

Question 1: Is the Nagata automorphism (or any polynomial automorphism) over a finite field non-tame?

The proof of Umirbaev-Shestakov only works in characteristic zero, hence the above question is still very much open.

Subproblem A: Which bijections are images of a polynomial automorphism?

There exists a canonical map $\pi_m:GA_n(\mathbb{F}_q)\rightarrow Bij(\mathbb{F}_r^{\,n})$ where $r=q^m$. In the paper [14] I study the case m=1, n≥2 and prove that π_1 is surjective if q is odd or q=2, and $\#Bij(\mathbb{F}_q^{\,n})/\#\pi_1(TA_n(\mathbb{F}_q))=2$ if $q=2^m$, m≥2. This induced the conjecture: *do there exist bijections in* $\pi_1(GA_n(\mathbb{F}_4))$ *which are odd permutations of* $(\mathbb{F}_4)^n$, *where* n≥3? By [8], such



The bijection $\pi_m(X+Y^2,Y)$ on $(\mathbb{F}_3)^2$.

an example would automatically be non-tame, and give a much simpler proof of the existence of non-tame automorphisms than Umirbaev-Shestakov. Over the years this has inspired many people to experiment with (known) examples, or try to apply a method from outside of AAG to conclude that $\pi_1(GA_n(\mathbb{F}_4))=\pi_1(TA_n(\mathbb{F}_4))$, but so far nothing worked.
Recently I took this research to a different level by investigating the case m ≥2. For, it may be that $\pi_1(GA_2(\mathbb{F}_q))=\pi_1(TA_2(\mathbb{F}_q))$, but $\pi_m(GA_2(\mathbb{F}_q))\neq\pi_m(TA_2(\mathbb{F}_q))$. I recently proved the (to me surprising) result that $\pi_m(GA_2(\mathbb{F}_q[X_3]))=\pi_m(TA_2(\mathbb{F}_q[X_3]))$ for any m and q, showing that for N the Nagata automorphism, $\pi_m(N) \in \pi_m(TA_2(\mathbb{F}_q[X_3])$. The research in this direction needs a new idea.
Here is one:

- Fix a tame polynomial automorphism σ of length n (i.e. a composition of at most n affine and n triangular maps).
- In case n≥2, show that for m>>n, $\pi_m(\sigma)$ has "chaotic" behavior.

This approach seems feasible for $TA_2(\mathbb{F}_q[X_3])$. And since $\pi_m(N)$ shows very orderly behavior, it is proven that N is non-tame.

But, more importantly, in attempts to catch this chaotic behavior, we come to a very **interesting link with (analytic) number theory**, which is interesting even without the above application:
Subproblem B: can we capture properties of automorphisms in zeta-like functions?
One possibility: associate to F an Artin-Mazur zeta-function like

$$\zeta_F(z) = \exp \sum_{k=1}^{\infty} \#\mathrm{Fix}(F^i)\frac{z^i}{i} .$$

For example, considering Nagata's automorphism N over $\mathbb{F}_q$ in characteristic p, then

$$\zeta_N(z)=(1-z)^{-q}(1-z^p)^{\frac{-q}{p}} .$$

Subproblem C: going from $GA_n(R)$ *to* $GA_n(\mathbb{F}_p)$ *and back.* This approach is an important part of the proof by Belov-Kontsevich, and apparently can be quite powerful. The point is to understand properties of maps over $\mathbb{Z}$ (or a finitely generated $\mathbb{Z}$-algebra R) by examining the map modulo almost all primes p (or maximal ideals $\mathfrak{m}$ in R). Important cases are R= $\mathbb{C}$, R= $\mathbb{Z}$.
Subproblem D: Find the Jacobian Conjecture over finite fields. The Jacobian condition det(Jac(F)) = 1 is a shorthand way of writing down many equations on the coefficients of a polynomial automorphism. In characteristic p these equations are not sufficient to imply being an automorphism (as the 1-variable example X^1+X^p shows). But, for each given p and n, they do exist and can be (heuristically) computed! The goal is to find these equations, and (1) provide an alternative to Adjamagbo's Jacobian Conjecture in characteristic p, and (2) have formulas that can help in applications to pick "random" automorphisms or permutation polynomials.

Before I end this topic, let me point out that underneath all the above questions, there is a meta-goal which transcends these questions:
Goal: build a good theoretical foundation of polynomial maps over finite fields.

Ph.-D project I:
This project will benefit a lot from the databases which Roel Willems computed for his Ph.-D. project under my guidance. Possible topics are:
Mock automorphisms.
In [27] I introduce the so-called mock automorphisms, which are polynomial maps F: $(\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n$ which are (1) bijections, (2) satisfy det(Jac(F)) in $\mathbb{F}_q^*$. The set of such maps is closed under composition (not a group obviously), and acts as an "in between" for multivariate permutation polynomials and polynomial automorphisms, while perhaps

being easier to understand as either. There are two interesting questions, which require initial computer calculations to see a pattern, and should both be feasible in dimension 2 at least:

(1) Classify the mock automorphisms modulo polynomial automorphisms,
(2) Classify permutation polynomials modulo mock automorphisms.

(Computer) experiments on zeta-functions associated to automorphisms. See subproblem B. Obviously, the goal is not only to discover interesting behavior by experiments, but also attempt to prove them.
Analysis of finite groups associated to $\pi_m(TA_n(\mathbb{F}_q))$.
One of my recent results is showing that

$$\pi_m(<Aff_n(\mathbb{F}_q),e>)=\pi_m(TA_n(\mathbb{F}_q))$$

where e is a specific automorphism, a result related to a theorem of H. Derksen. (This theorem could even be useful for practical applications.) Essentially, this assignment is to fix an interesting subgroup H of $TA_n(\mathbb{F}_q)$, and study $\pi_m(H)$.
Subproblem C over $\mathbb{Z}$*:* Characterize properties of elements in $SA_n(\mathbb{Z})$ by their properties modulo each prime p.
Subproblem D can be (partially) assigned to the Ph.-D. student too.

Topic II: LF automorphisms
In the paper [16] I introduced the class of so-called *Locally Finite Polynomial Endomorphisms* (short LF endomorphism or LF automorphism). This class is defined as the set of endomorphisms F which are "zero of a polynomial $P_F(T):=T^n+a_{n-1}T^{n-1}+\ldots+a_1T+a_0$", which means that $F^n=-a_{n-1}F^{n-1}-\ldots-a_1F-a_0I$ (where a_i in $\mathbb{C}$, and $F^m=F\circ F\circ\cdots\circ F$). Being an LF map is very restrictive, but it turns out that most of the interesting automorphisms are in this class: linear, affine, triangular maps, all involutions, the Nagata automorphism, exponents of locally nilpotent derivations, quasi-translations (see [17]), etc. etc.
The research will mainly focus on the set $LF_n(R)$ of LF *automorphisms.* (R a ring, but often R= $\mathbb{C}$. Picking R= $\mathbb{F}_q$ links this topic with topic I.) The group generated by $LF_n(R)$ is denoted by $GLF_n(R)$.
Link with complex analysis: One can define LF holomorphic maps (in several variables) in a similar way. This gives rise to the larger, holomorphic sets $LF_n\{\mathbb{C}\}$, $GLF_n\{\mathbb{C}\}$ defined similarly. Some questions we pose here can be posed for these sets too, and in some sense these groups might be easier to understand (for having more generators!).
Question 2: Understand the groups $GLF_n(\mathbb{C})$, $GLF_n\{\mathbb{C}\}$ in terms of their generators.
The set $LF_n(\mathbb{C})$ is closed under conjugation by $GA_n(\mathbb{C})$, which is special (the set $TA_n(\mathbb{C})$, for one, is not when n≥3). And in fact, in my opinion, the set $LF_n(\mathbb{C})$ is the most natural answer to the Generator Problem:
Subproblem A: Show that $GLF_n(\mathbb{C})=GA_n(\mathbb{C})$.
A harder problem than question 2, in general! I do think, however, that it is possible to solve the following important subcase:
Subproblem B: Show that $GLF_2(\mathbb{C}[X_3])=GA_2(\mathbb{C}[X_3])$.
In [18] results are shown that can be a first step to a solution of this problem.
Links with dynamics surface since LF automorphisms behave much more like linear maps than regular automorphisms – it makes sense to talk about their eigenvalues, for one. Another link is the following:
Subproblem C: Show that F *in* $LF_n(\mathbb{C})$ *implies that* F *is a time-one map of a* $\mathbb{C}$ *–flow.*
I can prove this for many F's, when the eigenvalues of F have no torsion (unpublished), but some interesting cases, like involutions, do have torsion.
Find links between the minimum polynomial $m_F(T)$ *and* F *having a fixed point.*
Experiments have already shown that there is a relation with $m_F(1)=0$. This problem will definitely be solvable (but still interesting) for the case n=2.

<u>Topic III: Modern Invariants</u>
Next to the topological invariants for (affine) spaces, in recent years the Makar-Limanov invariant and Derksen invariant (short: ML and D invariants) have surfaced. There are interesting connections with geometric properties, like A_1-fibered surfaces (see [19]), and flexible varieties (see [20]). A key issue seems to be the understanding of the ML and D invariants, and when they distinguish the same surfaces. (One of my contribution was finding the first examples where the D and ML invariants truly differ.) It is an interesting and important problem to pinpoint what exactly these two invariants measure. I want to close the gap between these two invariant by finding "better" examples where the invariants differ, and find conditions under which the invariants are the same.

Next to that, there's also the issue that one hopes to improve the invariants. For example, one could consider only the invariants of faithful $(G_a)^2$-actions (corresponding to commuting locally nilpotent derivations, see [21, 22]) in stead of plain G_a-actions. That is quickly defined, but the issue is the following:
Question 3: For a fixed integer m, is the intersection of invariants of $(G_a)^m$ actions computable in some interesting cases?

<u>Topic IV: Poisson algebras</u>
A Poisson algebra is an associative algebra endowed with a Lie bracket [-,-] that is also a derivation. For this proposal, we will only consider algebras which are commutative rings, and in particular, the case where the ring is a polynomial algebra in 2n variables, i.e. we have the ring $P_n:=k[X_1,\ldots,X_n,Y_1,\ldots,Y_n]$. The interest in this object is sparked by both the results of Belov-Kontsevich and Umirbaev-Shestakov: both use Lie brackets and Poisson algebras, which was not (often) heard of before in AAG. Poisson algebras are a vast and important topic in **mathematical physics** and related fields. In fact, if one checks the MathSciNet site, there are many, many papers on Poisson algebras, but studying Poisson algebras from a commutative algebra viewpoint has been mostly neglected. However, the puzzling fact that the two most fabled recent results in Affine Algebraic Geometry heavily use these algebras, simply *cries out* for more research!
Question 4: What is the automorphism group of P_n?
The automorphism group of P_n is a subgroup of $GA_{2n}(k)$ preserving the bracket. There are many automorphisms here, as the bracket can have many shapes. The standard bracket on P_n, which is the bracket $[X_i,Y_j]=\partial_{ij}$ and $[X_i,X_j]=[Y_i,Y_j]=0$, yields the symplectic algebra S_n. Now the statement "Endomorphisms of S_n are always automorphisms" is equivalent to the Jacobian Conjecture (!). However, experiments showed that if one takes a nonstandard bracket on P_n then the set of automorphisms becomes smaller, but the set of noninvertible endomorphisms grows. This gives rise to the:
<u>*Subproblem A: Investigate if the set of endomorphisms of P_n is (approximately) equal in size for different brackets.*</u>
The n=1 case is definitely solvable. In fact, it means solving the following problem:
<u>*Subproblem B: Determine the subgroup of $GA_2(k)$ preserving*</u> $[X_1,Y_1]=X_1$
Note that above, I have left k to be as general as possible. It is interesting to study all these questions for different fields. In fact, it is very plausible that getting a result over finite fields (topic I!) yields a result over $\mathbb{C}$ and other fields, as is done in Belov-Kontsevich.

<u>Topic V: Information theoretic cryptography</u>
It has always been one of my goals to find an application of polynomial automorphisms outside of pure mathematics. Applying polynomial maps to cryptography is not new: Moh introduced [23] a public key cryptosystem based on the computational difficulty of inverting a polynomial map. My approach is different:
Question 5: How can polynomial automorphisms be used in symmetric key cryptography?

Recently, I wrote a preprint [25], giving an alternative way of doing session-key generation in a symmetric key setting. I introduce a scheme where the secret key is a polynomial automorphism. Interestingly, this work gave rise to some useful and interesting questions that could fit perfectly under topic I, and which has shown to me that doing a combination of very "pure" mathematics combined with "applied" mathematics is very stimulating for both[1]!

There are several possibilities for other applications:

- Designing random number generators: since polynomial automorphisms generate at least half of all bijections, picking an "intelligent" representation of a "random" polynomial map is an excellent way of generating such a random number generator. (See [26] for a similar application.)
- In multi-party computation, several users share a secret. There are possibilities to design certain protocols using polynomial automorphisms. Simply put, if a protocol uses maps, it is sometimes possible to let the maps be polynomial maps. (An inspiration here is the Blom scheme.)

Post-Doc project:
In my opinion, quality of post-doc is more important than fixing the topic. Hence, instead of restricting the post-doc to a specific outlined project (as I did for the Ph.-D.) I will give the post-doc the liberty of choosing between the above topics and problems, and work closely with him/her.

Originality, innovative methods and topics.
The underlying goal of this proposal is to carry AAG away from its standard subjects and thought patterns, and thus it inherently *has* to be innovative:

- Polynomial maps over finite fields is almost unresearched but timely.
- Researching Poisson algebras as an object in *commutative algebra* is a surprisingly novel approach to an often researched object.
- Locally finite polynomial automorphisms as a subject, was a novel subject of my VENI grant. My viewpoint has changed, though: connections with dynamical systems and real or complex analysis.
- Applying polynomial *auto*morphisms to symmetric key cryptography: to my knowledge this proposal (and my preprint [25]) is the first document that even mentions it!

Why me?
Topics I, II and V have been initiated by me. Especially topic I has attracted quite a few researchers (also from outside of AAG, which I like a lot!), and from that the applications in topic V have just surfaced. If topic V[2] gets the boost as intended through this proposal, this could have quite a **large impact** on my research field and the people working in it. If I don't get the opportunity to develop this, however, it will never happen.

Plan of work
A strong (and for me exciting!) point of my work plan is my explicitly planned collaboration with:[3]
Prof. U. Umirbaev, Wayne State University, USA on topic I and II mainly. Umirbaev is a rising star in our field: his result together with Shestakov is no coincidence, and I think that our collaboration will be mutually beneficial in getting concrete results.

[1] And thus perhaps showing that the difference between pure and applied is relative.
[2] See also the paragraph 2b !
[3] They are aware of my research plan and agreed to my plan of visiting & inviting them.

Prof. L. Makar-Limanov, Wayne State University, USA on topic III and IV. Makar-Limanov is probably one of the best known researchers in AAG, and has many ground-breaking results to his name.

Timeline:

	PI	Ph.-D	Post-Doc	Other
2012	I			
2013				V1
2014	T1			C
2015		T2		
2016				V2
2017				

Legenda:
Grey = hiring period.
I: Visit the companies mentioned under **2b**.
T1: Visit to Makar-Limanov & Umirbaev
T2: Ph.-D. students stay abroad for 3-6 months. Very suitable are several places in Michigan (USA) or Dijon (France), but many other options are possible.
V1&V2: Makar-Limanov and Umirbaev visit me for 3 months each.
C: Organization of conference/summer school at TUE on AAG and its applications

<u>(Planned) national collaborators</u>**:**

- <u>Eindhoven:</u>It has my preference to locate the project at the TUE, due to the proximity to the companies, the large and well-known cryptography/security group (approx. 30 people, o.a. de Lange/Tilborg/Schoenmakers/de Weger/Etalle/Skoric) and the Discrete Algebra and Geometry group (Cuypers/Cohen/Draisma/Blokhuis/Sterk). I will benefit from them mainly on topic I & V.
- <u>Industry:</u> G-J.Schrijen (Intrinsic-ID), Tom Kevenaar (Priv-ID)
- <u>National</u>: H. Peters (UvA) on topic II, Van den Essen and group (RU) on topics I,II,III.

The project can be connected with the clusters DIAMANT and GQT.

<u>International collaborations</u>: Next to Makar-Limanov and Umirbaev, the list in **4h** is an indication of people I could collaborate with. In particular, I will most probably visit[4] the research groups in Bochum (Flenner, Winkelmann, Huckleberry), Dijon (Dubouloz, Moser), Basel (Kraft, Blanc, Poloni, Vénéreau), Zurich (Rosenthal), St. Louis (Wright, Kumar), Ann Arbor (Derksen).

[4] Except for the people at Bochum, these have not been contaced directly about the project.

2b. Research Impact

Short term: Applications in industrial cryptography
I am very happy with, and proud of, the fact that my proposal holds the whole spectrum of pure, theoretical mathematics, to actual applications in industry. Note that I have experience working in this industry (2004/2005), and that my VENI-grant already had a slight idea to seek out such an application, but was hampered by lack of a theoretical foundation. Indeed, laying out this foundation has turned out to be fruitful, and the time is right to put a more concrete emphasis on such applications.

I have contacts with the following companies (between brackets contact person and main topic):
PRIV-ID (Tom Kevenaar, fingerprinting), INTRINSIC-ID (Geert-Jan Schrijven, chipcard crypto & PUFs). The plan of work is to visit these companies, listen to their needs, and see if I can make a contribution to their work by helping them solve their problems, and in the best case, make patents. In my contacts with them so far it has become clear that my work may provide solutions for some of their problems:

PRIV-ID seeks methods to make hash functions which have a property which seems to contradict the essence of cryptographic hash-functions: Input values which differ only slightly (fingerprints!) should have a high chance of having a similar output, while input values which differ "more than slightly" have completely unrelated outputs. One of the only ways in which they were able to do this, is by polynomial maps. Interestingly, I have an idea using a result hidden in [16, page 456-457] (topic II) which, if generalized, can be of help here!

INTRINSIC-ID mainly seeks ways in which to enhance existing algorithms' speed while keeping (almost the same) security (to be more precise: using less *gates*, so-called "low-footprint crypto"). They have shown interest in [25], which should be compared to other existing options, though. Another option is the following: in some of their applications, an exponentiation in a discrete log setting is used. It may be replaced by a suitable (multivariable) permutation polynomial.

There are also possibilities of applying my work to *low-power cryptography* (where at least one of the devices is low-power, like a modern RFID tag), but I am currently unaware of a Dutch company doing this actively (except, to a minor degree, the above two companies).

Long-term impact of the overall research
Next to the above, very concrete application in cryptography, there is an underlying thought pervading through this research proposal (which may not be obvious from the very theoretical approach). As said, linear maps are omnipresent in mathematical applications. In some cases, they are not used because they are *linear,* but because they are *well-understood* automorphisms of n-space. In those cases it is possible to use a larger class of automorphisms, like holomorphic, or polynomial, but often the problem here is this word "*well-understood".* Using the nonlinear maps can be very difficult or ad-hoc.
If polynomial automorphisms would be (almost) as easy to use as linear maps, then they could be used in practice to get better results.
The above statement is not just some "grant proposal talk" - I will describe an explicit example from my own work in industry: we were working on a device/method to recognise fingerprints of various persons. Fingerprint measurements were coded as a list of parameters (and hence elements of a vector space). Measurements taken of one person at different times could differ quite a bit. In order to distinguish persons, lines were drawn between individuals and their measurements. However, in different

polynomial coordinate systems it was possible to draw lines that were much better, significantly improving the false-rejection and false-accept rates. However, finding such a coordinate system was frustrated by the lack of a decent theory on such automorphisms.

Three other examples of applications are:
1. Volume-preserving maps in physics.
- Incompressable fluids: any mixing of the fluid is a continuous map $\mathbb{R}^3 \rightarrow \mathbb{R}^3$. In fact, an interesting model for mixing two fluids can be given by the composition of two locally finite maps (coming from flows).
- Quantum fluids: highly compressed electrons at absolute zero. Similar to the above.
- Canonical transformations. Volume-preserving transformations of the phase space.

Here, there is no restriction on the type of maps (i.e. they can be analytical) but polynomial maps are automatically volume-preserving (after a linear transformation), making them easy to work with. While preparing this proposal I felt that here is a future direction of research for me: consulting the experts in physics and seeing how I can help their problems along. (I do already have contacts with a few, like B. Skoric (TUE), M. Baake (Bielefeld), W. van Suijlekom (RU)).
2. Approximating functions of measured data. Uniformly, with respect to some metric. Doable (but not trivial) if the function can be an endomorphism, but what if it is supposed to be injective, or even an automorphism? For example, measured data can come from independent stochasts, completely scrambled in the measure space, with some noise on top. In that case there is an injective map from the original stochasts to the measurement space, and then an approximation should be injective itself.
3. Another problem that surfaced a few times in applications (for example cryptography) is: find a (in some sense) random automorphism. It is efficient to pick a random linear automorphism: pick a random linear map, and check its determinant, which is nonzero most of the time. For polynomial automorphisms there are no useful methods to pick a random polynomial automorphism. In fact, this theoretical problem is so hard, that I did not even mention it in the theoretic part of the proposal (though subproblem D of Topic I gives some footholds).

Let me point out two of the central issues of this void in knowledge that I address:
- Many computer applications will use polynomial maps over finite fields. This proposal paves the way for any such application.
- LF maps are much more similar to linear maps than generic automorphisms, making them a possible first candidate for applications.

2c. Number of words used: section 2a 3989 words (max. 4000 words)
NOTE: Microsoft Word counts 4011 words, but has some trouble with certain mathematical formulas.

Number of words used: section 2b 1000 words exactly! (max. 1000 words).

2d. Any other important remarks with regard to this application

2e. Literature references

[1] Cima, Anna; van den Essen, Arno; Gasull, Armengol; Hubbers, Engelbert; Mañosas, Francesco, *A polynomial counterexample to the Markus-Yamabe conjecture*. *Adv. Math.* 131 (1997), no. 2, pp. 453-457.
See also http://www.math.unl.edu/~gmeisters1/papers/HK1996.pdf

[2] Many papers, two of them:

- Daigle, Daniel; Freudenburg, Gene. *A counterexample to Hilbert's fourteenth problem in dimension 5*. *J. Algebra* 221 (1999), no. 2, pp. 528--535.
- Kuroda, Shigeru. *A counterexample to the fourteenth problem of Hilbert in dimension four*. *J. Algebra* 279 (2004), no. 1, 126--134.

[3] Belov-Kanel, Alexei; Kontsevich, Maxim. *The Jacobian conjecture is stably equivalent to the Dixmier conjecture*. *Mosc. Math. J.* 7 (2007), no. 2, pp. 209--218, 349.

[4] Borisov, Alexander; Sapir, Mark. *Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms*. Invent. Math. 160 (2005), no. 2, 341–356.

[5] Karel Dekimpe, Paul Igodt *Polycyclic-by-finite groups admit a boundeddegree polynomial structure.* Invent.Math. 291, 121-140 (1997)

[6] Shestakov, Ivan P.; Umirbaev, Ualbai U. *Poisson brackets and two-generated subalgebras of rings of polynomials. J. Amer. Math. Soc.* 17 (2004), no. 1, 181—196.
and
Shestakov, Ivan P.; Umirbaev, Ualbai U. The *tame and the wild automorphisms of polynomial rings in three variables*. *J. Amer. Math. Soc.* 17 (2004), no. 1, 197--227 (electronic).

[7] Several results:
- Berson, Joost; van den Essen, Arno; Wright, David. *Stable Tameness of Two-Dimensional Polynomial Automorphisms Over a Regular Ring.* arXiv:0707.3151v8
- Maubach, Stefan; Poloni, Pierre-Marie. *The Nagata automorphism is shifted linearizable*. J. of Algebra, 321 (3), pp. 879-889, Feb 2009
- Edo, Eric ; van den Essen, Arno; Maubach, Stefan; *A note on k[z]-automorphisms in two variables*, to appear in J. Pure Appl. Alg.

[8] Adjamagbo, Pascal Kossivi; van den Essen, Arno. *A proof of the equivalence of the Dixmier, Jacobian and Poisson conjectures. Acta Math. Vietnam.* 32 (2007), no. 2-3, 205--214.
and
Bavula, V.V.; *The Jacobian Conjecture implies the Dixmier Problem*, arXiv:math/0512250v1

[8] L. Makar-Limanov, L. *On the hypersurface x+x^2y+z^2+t^3=0 in C^4 or a C^3 -like threefold which is not C^3.* Israel J. Math., 96(1996), 419-429

[9] Crachiola, A. ; Maubach, S.; *The Derksen invariant vs. the Makar-Limanov invariant*. Proc. Amer. Math. Soc. 131 (2003), no.11. 3365-3369.

[10] Finston, D., Maubach, S., *The Automorphism Group of Certain Factorial Threefolds and a Cancellation Problem.* Israel J. Math 163 (2008) No.1

[11] Dubouloz, Adrien; Moser-Jauslin, Lucy; Poloni, Pierre-Marie, *Non cancellation for smooth contractible affine threefolds*. eprint arXiv:1004.4723

[12] Two papers:
- Adjamagbo, Pascal Kossivi; van den Essen, Arno. *A proof of the equivalence of the Dixmier, Jacobian and Poisson conjectures*. Acta Math. Vietnam. 32 (2007), no. 2-3, 205--214.
- Bavula, V.V.; *The Jacobian Conjecture implies the Dixmier Problem*. arXiv:math/0512250v1

[13] six papers and preprints:
- P. Nousiainen, *On the Jacobian Problem in positive characteristic*, Pennsylvania State Univ. , unpublished preprint (1981)
- K. Adjamagbo, *On seperable algebras over a U.F.D. and the Jacobian Conjecture in any characteristic*, Proceedings of the conference `Invertible Polynomial Maps', 89-104
- K. Adjamagbo, H. Derksen, A. van den Essen, *On polynomial maps in positive characteristic and the Jacobian Conjecture,* unpublished, report 9208, Univ. of Nijmegen, (1992)
-Roberts, John A. G.; Vivaldi, Franco. *Signature of time-reversal symmetry in polynomial automorphisms over finite fields.* Nonlinearity 18 (2005), no. 5, 2171--2192.
- Borisov, Alexander; Sapir, Mark. *Polynomial maps over finite fields and residual finiteness of*

mapping tori of group endomorphisms. Invent. Math. 160 (2005), no. 2, 341--356.
- Borisov, Alexander; Sapir, Mark. *Polynomial maps over p-adics and residual properties of mapping tori of group endomorphisms.* arXiv:0810.0443v1
(Note that the following two papes are on polynomials in *one* variable, so they are NOT on the indicated topics: -Batra, Anjula; Morton, Patrick. *Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. I. Rocky Mountain J. Math.* 24 (1994), no. 2, 453--481. -Batra, Anjula; Morton, Patrick. *Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. II. Rocky Mountain J. Math.* 24 (1994), no. 3, 905--932.)

[14] Maubach, Stefan. *Polynomial automorphisms over finite fields*. *Serdica Math. J.* 27 (2001), no. 4, 343--350.

[15] Furter, Jean-Philippe; Lamy, Stéphane, *Normal subgroup generated by a plane polynomial automorphism.* eprint arXiv:0910.1616

[16] Furter, Jean-Philippe; Maubach, Stefan. *Locally finite polynomial endomorphisms*. *J. Pure Appl. Algebra* 211 (2007), no. 2, 445--458.

[17] de Bondt, Michiel. *Quasi-translations and counterexamples to the homogeneous dependence problem*. *Proc. Amer. Math. Soc.* 134 (2006), no. 10, 2849--2856 .

[18] Furter, Jean-Philippe; Maubach, Stefan. *A Characterization of Semisimple Plane Polynomial Automorphisms.* arXiv:0804.2157v2

[19] Blanc, J., Dubouloz, A., *Automorphisms of A^1-fibered surfaces.* preprint (2009) arXiv:0906.3623

[20] Arzhantsev, I.; Flenner, H.; Kaliman, S.; Kutzschebauch, F.; Zaidenberg, M., *Flexible varieties and automorphism groups.* Preprint (2010) arXiv:1011.5375

[21] Maubach, S. *The commuting derivations conjecture*. J. Pure Appl. Algebra 179 (2003), No.1-2. 159-168.

[22] Derksen, Harm; van den Essen, Arno; Finston, David; Maubach, Stefan, *Unipotent group actions on affine varieties,* Journal of Algebra Volume 336, Issue 1, 15 June 2011, Pages 200-208

[23] Several papers, I give one:
Moh, T. *A public key system with signature and master key functions. Comm. Algebra* 27 (1999), no. 5, 2207--2222.

[24] One recent example of several:
Dubois, Vivien; Pierre-Alain Fouque, Pierre-Alain; Shamir, Adi; Stern, Jaques. *Cryptanalysis of SFLASH*. CRYPTO 2007: 1-12

[25] Stefan Maubach, *Triangular polynomial Z-actions on (F_p)^n,* arXiv:1106.5800

[26] Two papers:
- Ostafe, Alina; Shparlinski, Igor E. *Pseudorandom Numbers and Hash Functions from Iterations of Multivariate Polynomials.* arXiv:0908.4519v2
- Ostafe, Alina. *Pseudorandom vector sequences of maximal period generated by triangular polynomial dynamical systems.* Designs, Codes and Cryptography, volume 54, p. 1-14

[27] Maubach, Stefan; Willems, Roel. (Joint with R. Willems*) Polynomial automorphisms over finite fields: experimental results,* arXiv:1103.3363

Cost estimates

3a. Budget

(Calculated for starting date September 2012)

Staff costs per calendar year in k€ incl. surcharge									
Scientific Staff	FTE	nr of months	2012	2013 k€	2014 k€	2015 k€	2016 k€	2017 k€	TOTAL k€
Applicant	1	60	24.2	76.2	79.8	83.6	87.4	58.8	410.0
PhD student I	1	48	0.0	39.1	46.4	49.5	52.9	0.0	187.9
PostDoc	1	24	0.0	0.0	0.0	63.5	64.7	0.0	128.2
Non scientific staff (NWP)	FTE	nr of months	2012	2013	2014	2015	2016	2017	TOTAL k€
academic level	0								0
HBO/Bachelor-level	0								0
MBO/Foundation Degree-level	0								0
Non staff costs: (k€)			2012	2013	2014	2015	2016	2017	TOTAL k€
Give a description of the non staff cost, as detailed as possible									
Equipment			3	3					6
Travel costs: Generic budget Visit P.I to Wayne State Foreign stay Ph.D.			0.6	4	4 10	6 8	6	1.3	39.9
Visitor: Makar-Limanov Visitor: Umirbaev Conference/Summer school				10	 8		 10		28
TOTAL									800

3b. Indicate the time (in fte) you will spend on the research

1.0 fte

3c. Intended starting date

Approx. September 2012

3d. Have you submitted the same idea elsewhere or have you requested any additional grants for this project either from NWO or from any other institution?

Partly yes: I submitted a grant proposal having some overlap with this one for a Heisenberg stipendium with the German DFG. Obviously, I can only take either the Heisenberg or Vidi grant, so this is of no real consequence.

Curriculum vitae

4a. Personal details
Title(s), initial(s), first name, surname: Dr. S. J. (Stefan) Maubach
Male/female: Male
Date and place of birth: 29 december 1974, Heerlen, The Netherlands
Nationality: Dutch
Birth country of parents: Netherlands/Germany

4b. Master's ('doctoraal')
University/College of Higher Education: Radboud University
Date (dd/mm/yy): 01/09/1998
Main subject: Hilbert's 14th problem and related subjects.
Distinction: *Cum Laude* (highest possible)

4c. Doctorate
University/College of Higher Education: Radboud University
Date (dd/mm/yy): 22/09/2003
Supervisor ('Promotor'): F. J. (Frans) Keune
Co-supervisor: A. van den Essen
Title of thesis: Polynomial Endomorphisms and Kernels of Derivations

4d. Current employment
University Lecturer (approx. Assistant professor, high teaching load)
Tenure-track

4e. Work experience since completing your PhD
Specify per appointment: number of fte, tenured term ('vast') / fixed-term ('tijdelijk'), and supervisory responsibilities (if any).

		Position	**Employer**	
11-2003	04-2004	Replacement teacher	Merlet College Cuyk.	Fixed-term (approx. 0.7 fte)
05-2004	08-2005	Industrial researcher cryptography & security	Philips Research, CRYPTO cluster Eindhoven	Tenured (1.0 fte)
09-2005	08-2006	Assistant Professor Mathematics	University of Brownsville, Texas, USA	Tenure track (1.0 fte) *Academic*
07-2006	06-2010	VENI-PostDoc (.75 fte), Lecturer (.25 fte) **Supervision:** 1 Ph-D. student 1 Master's student 1 Bachelor student 2 projects	Radboud University	Fixed-term (1.0 fte) *Academic*
01-2010	05-2010	External lecturer (1 course)	Jacobs University Bremen	Fixed-term, unmeasured fte. *Academic*
09-2010		Lecturer	Jacobs University Bremen	Tenure track (1.0 fte) *Academic*

For the season 2007/2008 "Lecturer" is replaced by "Oberwolfach Leibniz Fellow".

4f. Man-years of research (as of October 2011)

11-2003 to 04-2004: 0.0 mfte (voluntary time spent: 0.18 mfte, not counted.)
05-2004 to 08-2005: 16months x 0.6 fte = 9.6 mfte (industrial research, approx. 60%, the other 40% being management)
09-2005 to 06-2006: 10months x 0.4 fte = 4.0 mfte (40% teaching, 20% management, 40% research)
07-2006 to 06-2010: 48months x 0.75 fte= 36.0 mfte (25% teaching/outreach, 75%research)
09-2010 to 10-2011: 13months x 0.2 fte = 2.6 mfte (80% teaching, 20% research)

52.2 mfte = **4.35 man-years of research**
Of which: 0.8 industrial
3.55 academic

4g. Brief summary of research over the last five years
(247 words; max. 250 words)

Main topics: Algebraic geometry, computer algebra, cryptography.

Much of my work is done in international collaboration (see the papers for names).

Algebraic varieties and group actions

I worked on the Makar-Limanov and Derksen invariants [8,11,16] as a tool to distinguish varieties. I used $(G_a)^2$ - actions to distinguish varieties from affine space [7,21]. I gave the 3-dimensional factorial counterexamples to the generalized cancellation problem [13,15].

Automorphisms and coordinates

I solved an important problem of Vénéreu in [10] on coordinates, by proving that $SGA_n(R[t]) \rightarrow SGA_n(R[t]/t^m)$ is surjective. In [12,17] I initiated the research to LF maps, classifying the dimension 2 case, and proving a Cayley-Hamilton-like theorem. In [17] I solved a problem posed by prof. Wlodzimierz Jelonek. In [19] I showed that Nagata's automorphism and others are not linearizable, but composed with particular linear maps it is. (Sort of a variant of Siegel's theorem.) This has close connections to the Markus-Yamabe problem. In [18] I gave, among others, a useful criterion on when f(x,y,z) is a coordinate.

Multivariate maps over finite fields and cryptography

In [3,25,26,27] I have laid out the first steps towards a theory on polynomial automorphisms over finite fields. In [24] I give an algorithm to efficiently compute preimages of polynomial maps, being of importance for public-key applications of polynomial automorphisms. In [25] I show that Nagata's automorphism and others over finite fields are indistinguishable from tame automorphisms when examining the bijections induced by them. In [27] I give a symmetric key application of polynomial maps.

4h. International activities

International collaboration (since July 2006)

As Oberwolfach Leibniz Fellow I invited guest researchers:
Stéphane Vénéreau (Basel, Switzerland),
Philippe Bonnet (Basel, Switzerland),
Anthony J. Crachiola (Saginaw, MI, USA),
Pierre-Marie Poloni (Dijon, France),
Jean-Philippe Furter (La Rochelle, France),
Takashi Kishimoto (Saitama, Japan),
David R. Finston (Las Cruces, NM, USA),
Eric Edo (Noumea, pacific France).

As post-doc RU I personally invited on Van Gogh + visitor's grants:
Leonid Makar-Limanov (Detroit, MI, USA),
Jean-Philippe Furter (La Rochelle, France),
Pierre-Marie Poloni (Dijon, France),
Adrien Dubouloz (Dijon, France),
Jakub Zygadlo (Krakow, France)

Visits over last 5 years to:
Heinz-Georg Quebbemann, Andreas Stein (Oldenburg, Germany),
Holger Brenner, Winfried Bruns (Osnabrück, Germany),
Christine Bessenrodt, Wolfgang Ebeling (Hannover, Germany),
Bettina Eick (Braunschweig, Germany),
Hubert Flenner, Alan huckleberry (Bochum, Germany),
Emilie Dufresne, Andreas Maurischat (Heidelberg, Germany)
Anthony J. Crachiola (Saginaw, MI, USA),
Leonid Makar-Limanov (Detroit, MI, USA),
Gene Freudenburg (Kalamazoo, MI, USA),
Michael Baake (Bielefeld, Germany),
Jaques Alev (Reims, France),
Adrian Dubouloz, Lucy Moser-Jauslin, and Pierre-Marie Poloni (Dijon, France),
David R. Finston (Las Cruces, NM, USA),
David Wright, Joost Berson, and Mohan Kumar (St. Louis, MO, USA),
Hanspeter Kraft and Stéphane Vénéreau (Basel, Switzerland),
Anna Cima, Armengol Gasull and Francesc Mañosas (Barcelona, Spain),
Charles Cheng (Rochester, MI, USA),
Vladimir Shpilrain (New York, NY, USA),

Presentations: I gave 46 presentations so far, you can find slides of almost all presentations since 2006 on my homepage. One (almost arbitrarily) selected presentation of each of the last five years:

2010: *Affine algebraic geometry and polynomial automorphisms.*
6 universities: University of Oldenburg, Technical university of Braunschweig, University of Hannover, University Oldenburg, Bochum University, University of Heidelberg.

2009: *Polynomial automorphisms, especially over finite fields.*
Institut Fourier, Grenoble, France.

2008: *Polynomial automorphisms over finite fields and locally finite polynomial maps.*
Institute Poincare, Paris

2007: *Commuting derivations on UFDs.*
Workshop on Affine Algebraic Geometry, Oberwolfach, Germany

2006: *Polynomial maps over finite fields and cryptography.*
Steven's institute, New Jersey, USA.

4i. Other academic activities

Teaching: Since 1998 almost continuously, including high-school teaching experience. Please consult my CV on my webpage for details on courses taught etc.: http://math.jacobs-university.de/maubach/cv.html

Supervising:
- Roel Willems (Ph.-D. graduated July 2011)
- Mart Kelder (Master's Thesis, 2010)
- Pim Heesterbeek & Edo van Veen (freshman project)
- Lorijn van Rooijen (Bachelor's Thesis, 2009)
- Aart Konijneberg &Julius Witte (freshman project)

Defense committee:
Joost Berson (sept. 2004)
Michiel de Bondt (July 2008)
Roel Willems (July 2011).

Referee:
I have refereed about 70 mathematical articles for international journals, among which: Compositio Mathematica, Transformation Groups, Journal of Pure and Applied Algebra, Proceedings of the AMS. I am a reviewer for Zentralblatt.

Conference organisation:
Main organizer of the conference: Automorphisms of Affine Spaces (6-10 July 2009). (40 participants, budget 14K)

Outreach:
I am very interested and fond of outreach activities towards high school students!
- Aug. 2006 – Jan. 2009: Head of outreach programs of mathematics, Radboud University.
- Aug. 2006 – Jan. 2009: Editorial staff of the *B4U Magazine* for high-school students.
- Jun. 2004 - Aug. 2005: Involved in Philips/Freudenthal Jet-Net project (increasing interest of secondary level students to scientific studies).

Academic service:
From November 2006 to October 2007 I was (founding!) president of the *Post-Doc Platform Nijmegen*. This organization was called to life to promote the interests of researchers and lecturers with temporary appointments at the Radboud University Nijmegen. Currently, it holds a (voted for) seat in the Works Council. See: http://www.ru.nl/rpnuk/

4j. Scholarships, grants and conference funding in last five years

(Reversibly ordered by date:)

AAS Conference: (13K)
(2009) Several grants (NWO, KNAW, Compositio, Diamant) for conference organization, totaling 13K euro.

NWO Visitor's Grant: (€ 1K)
A grant to invite prof. dr. Makar-Limanov. 1K euro.

Van Gogh cooperation grant: (€ 14K)
A joint grant for collaboration of me and Adrien Dubouloz (Dijon, France).

Oberwolfach Leibniz Fellowship: (€ 20K+, estimated)
A grant allowing me to stay for 3 months at the MFO in Germany, and invite up to one guest at any time.

VENI- grant: (€ 208K)
A similar (but smaller) grant as a Vidi.

List of publications

5a. Publications

International refereed journals

[22] (Joint with J. Berson, A. Dubouloz, J-Ph. Furter), *Locally tame plane polynomial automorphisms,* Accepted to Journal of Pure and Applied Algebra

[21] (Joint with H. Derksen, D. Finston, and A. van den Essen) *Unipotent group actions on affine varieties,* Journal of Algebra Volume 336, Issue 1, 15 June 2011, Pages 200-208

[20] (Joint with J-Ph. Furter) *A Characterization of Semisimple Plane Polynomial Automorphisms.* Journal of Pure and Applied Algebra 214 (2010) pp. 574-583

[19] (Joint with P-M. Poloni) *The Nagata automorphism is shifted linearizable,* Journal of Algebra 321 (2009) pp. 879-889

[18] (Joint with E. Edo and A. van den Essen) *A note on k[z]-automorphisms in two variables,* Journal of Pure and Applied Algebra 213 (2009) pp. 1197-1200

[17] (Joint with H. Peters) *Polynomial maps which are roots of power series,* Mathematische Zeitschrift 259 No.4 (2008) pp. 903--914

[16] (Joint with D. Finston) *Constructing (almost) rigid rings and a UFD having infinitely generated Derksen and Makar-Limanov invariant,* accepted to Canad. Math. Bull. (will appear in print in 2010)

[15] (Joint with D.Finston) *The Automorphism Group of Certain Factorial Threefolds and a Cancellation Problem*, Israel J. Math 163 No. 1 (2008) pp. 369-381

[14] (Joint with Nguyen Van Chau, as editors) *Some open questions on polynomial automorphisms and related topics*, Acta Math. Vietnamica 32, No. 2-3 (2007) pp. 303-318

[13] *On the methods to construct UFD counterexamples to a cancellation problem,* Acta Math. Vietnamica 32, No. 2-3 (2007) pp. 215-222

[12] (Joint with J-Ph.Furter) *Locally finite polynomial endomorphisms,* J. Pure Appl. Algebra 211 No. 2 (2007) pp. 445-458

[11] *Infinitely generated Derksen and Makar-Limanov invariant*, Osaka J. Math. 44 (2007) pp. 883-886

[10] (Joint with A.van den Essen, S.Vénéreau) *The Special Automorphism group of* $R[t]/(t^m)[X_1, \ldots, X_n]$ *and coordinates of a subring of* $R[t][X_1, \ldots, X_n]$, J. Pure Appl. Alg. 210 No.1 (2007) pp. 141-146

[9] (Joint with B. Škorić, T. Kevenaar, P. Tuyls) *Information-theoretic analysis of capacitive Physical Unclonable Functions,* J. Appl. Phys. 100, 024902 (2006).

[8] (Joint with A.Crachiola) *The Derksen invariant vs. the Makar-Limanov invariant,* Proc. Amer. Math. Soc. 131 no.11 (2003), pp. 3365-3369.

[7] *The commuting derivations conjecture,* J. Pure Appl. Algebra 179 No.1-2 (2003), pp. 159-168.
This paper ended in the **top 10** (9th) of most downloaded articles in 2003 of the Journal of Pure and Applied algebra.

[6] *The automorphism group of* $\mathbb{C}[t]/(t^m)[X_1, \ldots, X_n]$, Comm. Algebra 30 No.2 (2002) pp. 619-629.

[5] *The linearisation conjecture and other problems over nonreduced rings,* Comm. Algebra 30 No.4 (2002) pp. 1693-1704

[4] (Joint with J.Berson, A.van den Essen) *Derivations having divergence zero on R[X,Y]*, Israel J.Math. 124 (2001).

[3] *Polynomial automorphisms over finite fields,* Serdica Math. J. 27 No.4 (2001) pp. 343-350.

[2] *An algorithm to compute the kernel of a derivation up to a certain degree,* J.Symbolic Computation 29 No.6 (2000) pp. 959-970

[1] *Triangular monomial derivations on* $k[X_1, X_2, X_3, X_4]$ *have kernel generated by at most four elements,* J.Pure Appl. Algebra 153 No.2 (2000) pp. 165-170

Books:

(As editor, joint with H. Bass, N. Van Chau) Hanoi Lecture notes on Polynomial Automorphisms and the Jacobian Conjecture. Publishing House for Science and Technology, ISBN:776-2007/CXB/008-04/KHTNCN

Contributions to books:

RFID security: Cryptography and Physics Perspectives. Jorge Guajardo et. al (including Stefan Maubach),
book chapter in: RFID security – Techniques, Protocols, and System-on-chip design. Kitsos, Paris; Zhang, Yan (Eds.) 2009, XII, 446 p. ISBN: 978-0-387-76480-1

Quotations in books:

Some of my work is quoted in books not written by me:

The results of my master's thesis (a counterexample to Hilbert's 14th problem), written in January 1998, have never been separately published. The reason for this is: the result has been incorporated in the book of van den Essen, Polynomial maps and the Jacobian Conjecture, (Birkhauser Verlag,) pages 229 through 234.

The results of the papers [2] and [8] above have appeared in seperate paragraph each (8.4:"Maubach's algorithm" and 9.7.3: "Examples of Crachiola and Maubach") in the book "Locally Nilpotent Derivations and Ga-Actions" of G.Freudenburg, series "Encyclopedia of Mathematical Sciences", Springer Verlag.

Thesis:

Polynomial endomorphisms and kernels of derivations, Ph.-D. thesis, University of Nijmegen (2003)

Hilbert's 14^{th} problem and related topics. Master's thesis, University of Nijmegen (1998)

Other:

Submitted preprints:

[23] (Joint with A. Crachiola), *Rigid rings,* arXiv:1005.4949

[24] (Joint with M. de Bondt), *Computing preimages of polynomial maps,* arXiv: 1005.0288

[25] (Joint with R. Willems) *Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group,* arXiv: 0912.3387

[26] (Joint with R. Willems*) Polynomial automorphisms over finite fields: experimental results,* arXiv:1103.3363

[27] *Triangular polynomial Z-actions on (F_p)^n,* arXiv:1106.5800

International unrefereed conference proceedings:

(Joint with R. Brinkman and W. Jonker,) A lucky dip as a secure data store, WISSEC 2006

(Joint with B. Skoric and seven more authors,) ALGSICS - Combining Physics and Cryptography to Enhance Security and Privacy in RFID Systems, WISSEC 2006

Patents:

[P1] *Transponder System for Transmitting Key-Encrypted Information and Associated Keys.*
Inventors: Pim Theo Tuyls, Geert Jan Schrijen, Stefan Maubach, Boris Skoric, Antoon Marie Henrie Tombeur. Agents: NXP, B.V.;NXP INTELLECTUAL PROPERTY DEPARTMENT Assignees: NXP B.V. Origin: SAN JOSE, CA US IPC8 Class: AH04L908FI USPC Class: 380268

[P2] *Method and System for Authentication of a Low-Resource Prover.*
Inventors: Geert Jan Schrijen, Claudine Viegas Conrado, Stefan Jean Maubach. Agents: PHILIPS INTELLECTUAL PROPERTY & STANDARDS Assignees: KONINKLIJKE PHILIPS ELECTRONICS, N.V. Origin: BRIARCLIFF MANOR, NY US IPC8 Class: AH04L932FI USPC Class: 726 2

[P3] *Secure storage system and method for secure storing.*
Inventors: Richard Brinkman, Willem Jonker, Stefan Maubach. EP06113192.6.
US patent pending: PCT/IB2007/051374.

Research impact:
In case you have filled in question 2b (research impact), also indicate the publications, presentations, etc. you used to communicate earlier research results to (potential) users:
I communicated to the people mentioned in 2b: the result of [27] and, to a minor degree, the results of [3,25,26], as well as the algorithm in [24]. Then there are the results of [9, P1, P2, P3] which are on the application topic that I want to work on, but

using different methods. Finally, I gave a presentation in Oct. 2003, Philips High Tech Campus, Eindhoven, which resulted in me getting a job offer there!

Statements by the applicant

[x] **I have completed this form truthfully**

Name: Stefan Maubach

Place: Bremen

Date: 27 August 2011

Please submit the application to NWO in electronic form (PDF format is required!) using the Iris system, which can be accessed via the NWO website (www.nwo.nl/vi). The only exception to this rule concerns applications within the Medical sciences. The Medical Sciences division uses a similar system called ProjectNet, to which access is provided via the division's own website (www.zonmw.nl). For any technical questions regarding submission, please contact the Iris helpdesk (iris@nwo.nl).