From: (b) (6)
To: Miller, Carl A. (Fed)
Subject: Re: Multivariate crypto
Date: Friday, March 24, 2017 4:55:49 PM

Ha! Good luck finding a crypto reference that actually provides a straightforward answer. I'm not sure why it is, but researchers seem to tiptoe around a specific definition. Maybe it is because they are wanting to state confidently properties that are hard to verify computationally for specific schemes. In any case, it is easy to define.

First, consider an ideal I in a polynomial ring F[x1,...,xn] with a generating set G. The ideal I_{lt} generated by the leading terms in I is also generated by the leading terms of any Grobner basis of I. The set of leading terms of a Grobner basis of I will be a Grobner basis for I_{lt} as well, via the same calculation. Slightly generalizing this we can easily see that the Grobner basis calculation for G is paralleled in the calculation of a Grobner basis for the ideal generated by the homogeneous components of highest total degree in G, a homogeneous ideal. The degree of regularity of I is the (Hilbert regularity, index of regularity, Hilbert index, or degree of regularity, whichever term you can find) of the homogeneous ideal generated by the homogeneous components of highest degree in G. So it suffices to define degree of regularity for a homogeneous ideal.

Now, let I be a homogeneous ideal in F[x1,..xn]. We may view F[x1,..,xn] as a graded ring (graded w.r.t. Total degree) and then F[x1,..,xn]/I is also a graded ring, moreover, it is a graded F-vector space, V_0+V_1+..., where each V_i consists of the homogenous elements of degree i in the quotient. Then the Hilbert Series of the quotient is HS(t)=\sum_{n=0}^\infty dim_F(V_n)t^n. There is a classical result that there exists a polynomial called the Hilbert polynomial, HP(n) such that for some k, HP(n)=dim_F(V_n), that is, the coefficient of t^n in HS(t), for all n greater than or equal to k. This value k is the degree of regularity of the quotient, and by abuse of language we call it the degree of regularity of the homogeneous ideal (or in the general case, of the ideal of the previous paragraph).

You can find out much more by studying derivation of the Hilbert Polynomial directly.

Intuitively, the sequence dim_F(V_n) grows exponentially for n less than k, but then is given by a polynomial for higher values. This indicates that we are guaranteed that there are nontrivial syzygies among the leading terms of the G at this degree (though it could happen even sooner). This indicates that the first fall degree (a quantity that is dependent upon the specific algorithm for computing Grobner bases) is always bounded by the degree of regularity. Solving degree may not be so bounded, but seems to be in practice about the same.

I hope this helps!

Cheers,
Daniel

On Fri, Mar 24, 2017 at 3:27 PM Miller, Carl A. (Fed) <carl.miller@nist.gov> wrote:

> Hi Daniel –

I looked up some of the references we were talking about and they look good. One quick thing: can you point me to a formal definition of the degree of regularity? (I have some guesses as to what it means but I haven't found a definition yet.)

Thanks for your help on this, I appreciate it.

-Carl

———

Carl A. Miller

Mathematician, Computer Security Division

National Institute of Standards and Technology

Gaithersburg, MD

From: Daniel Smith (b) (6)
Date: Thursday, March 23, 2017 at 2:20 PM

To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>

Subject: Re: Multivariate crypto

The first thing that comes to mind is "Gr\"{o}bner Bases, Coding, and Cryptography" a Springer collection edited by Sala, Mora, Perret, Sakata, and Traverso. It has a quick and simple intro to Grobner bases and also a couple of articles dedicated to multivariate in the middle. It doesn't have to much of the theory that you need for explaining degree of regularity, but that is out of its scope. It is more computational and applied.

Cheers!

On Thu, Mar 23, 2017 at 12:51 PM, Miller, Carl A. (Fed) <carl.miller@nist.gov> wrote:

> Hi Daniel –
>
> That sounds great. I can imagine a talk where I would rehash how multivariate crypto works, explain the significance of the degree of regularity in multivariate crypto, and then spend the rest of the time on mathematical development.
>
> For multivariate crypto, Albrecht recommended a book by J. Ding et al. and also a book by D. Bernstein et al. For the algebra, I can think of "Commutative algebra with a view toward algebraic geometry" by D. Eisenbud, although that's more abstract than computational. Do you happen to know of any other references that might be good?
>
> Thanks!
>
> -Carl
>
> ——————
>
> Carl A. Miller
>
> Mathematician, Computer Security Division
>
> National Institute of Standards and Technology
>
> Gaithersburg, MD
>
> ---
>
> **From:** Daniel Smith (b) (6)

Date: Tuesday, March 21, 2017 at 7:46 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: Multivariate crypto

Hi, Carl,

I think that a great topic along these lines would be the degree of regularity (sometimes calles index of regularity) of an ideal. This quantity has practical significance in multivariate crypto because the degree at which nontrivial syzygies appear in Grobner basis calculations is bounded by this quantity and typically the maximum degree reached in a Grobner basis calculation is not significantly higher. It would be nice to address this directly instead of as a simple comment in a description of a particular scheme or attack. It is a value of critical importance that can be explained fairly simply just by explaining Hilbert series and the Hilbert polynomial.

Let me know if you think that would be a good topic. I'll try to think of something else that hits on algebraic geometry and is relevant and I'll let you know if I have any other useful thoughts.

Cheers!

Daniel