From: Miller, Carl A. (Fed)
To: (b) (6)
Subject: Re: Multivariate crypto
Date: Thursday, March 23, 2017 7:58:53 PM

Ok, thanks – I was able to find the book. I appreciate the help.

-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