From: Miller, Carl A. (Fed)
To: Petzoldt, Albrecht R. (IntlAssoc)
Subject: Re: Multivariate crypto
Date: Friday, January 27, 2017 5:16:07 PM

Ok, thanks a lot for the references. I may give a talk on this topic in the PQC seminar (it will be challenging to give a talk as a beginner in front of people who already know the subject, but I figure it's a good way to learn :)). Suggestions for topics are also welcome. Talk to you later!

-Carl

———

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Petzoldt, Albrecht R. (IntlAssoc)" <albrecht.petzoldt@nist.gov>
Date: Friday, January 27, 2017 at 11:54 AM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: Multivariate crypto

Hi,
The standard textbook about multivariate cryptography was written by Jintai Ding, Jason E. Gower and Dieter Schmidt and is entitled Multivariate Cryptography. As far as I know, it's based on a lecture Jintai gave once in Cininnati. The book is very mathematical and contains also detailed description of the attacks.

Another introductory overview on multivariate cryptography can be found in D. Bernstein, J. Buchmann and E. Dahmen: Post Quantum Cryptography. However, the chapter about multivariate cryptography in the 1st edition of this book is not written in a good style. Therefore I would recommend you the 2nd edition (it's not appeared yet, but I can send it to you if you are interested.) It's more an overview and does not contain all the mathematical details.

If you are interested further details or want to talk with me, please write me an email or directly step by in my room A362. I'd like to talk with someone about multivariate topics (so far I didn't find many potential co-workers here).

Best regards,
Albrecht

From: Miller, Carl A. (Fed)

Sent: Friday, January 27, 2017 11:02 AM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: Multivariate crypto

Hi Albrecht –

Thanks for your talk this morning! I have a question: do you know of a good reference to learn the basics of multivariate crypto? I have a background in finite fields (and algebraic geometry) so a mathematical treatment would be good. Talk to you later!

-Carl

———

Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD