From: Sonmez Turan, Meltem (Assoc)
To: Perlner, Ray A. (Fed); Dworkin, Morris J. (Fed)
Subject: RE: Reading Club talk June 8
Date: Thursday, May 26, 2016 2:25:42 PM

Thanks Ray and Morrie!

From: Perlner, Ray (Fed)
Sent: Thursday, May 26, 2016 11:07 AM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Subject: RE: Reading Club talk June 8

Thanks Morrie.
Meltem,
the abstract is correct, but I noticed that I didn't include the title with the abstract, so here it is:

Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme

From: Dworkin, Morris J. (Fed)
Sent: Thursday, May 26, 2016 11:03 AM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Fwd: Reading Club talk June 8

Hi, Meltem,
Ray already sent me his abstract, below.
Morrie

> Begin forwarded message:
> **From:** "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
> **Subject: Reading Club talk June 8**
> **Date:** May 23, 2016 at 9:07:01 AM EDT
> **To:** "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
> Here's the abstract:
>
> In the last few years multivariate public key cryptography has experienced an infusion of new ideas for encryption. Among these new strategies is the ABC Simple Matrix family of encryption schemes which utilize the structure of a large matrix algebra to construct effectively invertible systems of nonlinear equations hidden by an isomorphism of polynomials. The cubic version of the ABC Simple Matrix Encryption was developed with provable security in mind and was published including a heuristic security argument claiming that an attack on the scheme should be at least as difficult as solving a random system of quadratic equations over a finite field.
> In this work, we prove that these claims are erroneous. We present a complete key recovery attack breaking full sized instances of the scheme. Interestingly, the same attack applies to the quadratic version of ABC, but is far less efficient; thus, the enhanced security scheme is less secure than the original.
>
> -----Original Message-----
> From: Perlner, Ray (Fed)

Sent: Wednesday, May 18, 2016 1:50 PM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: RE: Reading Club talk June 8

June 8th is fine. If I haven't sent an abstract by the 25th, please remind me and I'll send it.

-----Original Message-----
From: Dworkin, Morris J. (Fed)
Sent: Wednesday, May 18, 2016 1:04 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Reading Club talk June 8

Hi, Ray,

Last week, I asked you if you could present your recent work with Daniel and Dustin to the Reading Club.
The date I had in mind was June 8, three weeks from today. If you're still willing and able, please send an abstract by May 25 for us to forward to the emailing list.
Thanks,

Morrie