From: Perlner, Ray (Fed)
To: CRYPTO-CLUB
Subject: RE: Reminder: Crypto Reading Club - June 8
Date: Wednesday, June 8, 2016 9:47:00 AM
Attachments: KRACCABCSMES.pptx

Slides

From: crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
Sent: Tuesday, June 07, 2016 12:06 PM
To: CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
Subject: [Crypto-club] Reminder: Crypto Reading Club - June 8

Hi everyone,

I would like to remind you that tomorrow Ray Perlner is giving a talk titled "Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme".

Date: June 8th, 2016
Place: Building 222 B341
Time : 10:00AM-12:00PM
Regards,
Meltem

From: crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
Sent: Thursday, June 2, 2016 1:31 PM
To: CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
Subject: [Crypto-club] Crypto Reading Club - June 8

Hi everyone,

Our next crypto reading club is scheduled on June 8th. Ray Perlner is giving a talk titled "Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme".

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.

Date: June 8th, 2016
Place: Building 222 B341
Time : 10:00AM-12:00PM
Regards,
Meltem