From: Moody, Dustin (Fed)
To: (b) (6)
Subject: Fw: FW: SAC 2016 notification for paper 104
Date: Wednesday, August 17, 2016 7:38:51 AM

From: Daniel Smith (b) (6)
Sent: Wednesday, June 29, 2016 3:50 PM
To: Moody, Dustin (Fed); Perlner, Ray (Fed)
Subject: Fwd: FW: SAC 2016 notification for paper 104

Congrats, the paper is accepted. Let's wait to see referee comments before changing more that clear errors.

Cheers,
Daniel

---------- Forwarded message ----------
From: **Smith-Tone, Daniel (Fed)** <daniel.smith@nist.gov>
Date: Tuesday, June 28, 2016
Subject: FW: SAC 2016 notification for paper 104
To: (b) (6)

From: SAC 2016
Sent: Tuesday, June 28, 2016 3:34:28 PM (UTC-05:00) Eastern Time (US & Canada)
To: Smith-Tone, Daniel (Fed)
Subject: SAC 2016 notification for paper 104

We are pleased to inform you that your paper has been selected to be presented at SAC 2016. This year, SAC had 100 submissions and we were only able to accept less than 30.

Now that your paper has been accepted, you must update your paper for the pre-proceedings to be distributed at the conference. Following the conference, finalized versions of the papers will be published as a proceedings in the Springer Lecture Notes in Computer Science series. Reviewers’ comments on your paper are attached and you must consider these in updating your paper.

Pre-proceedings: The pre-proceedings version (to be distributed electronically at the conference) is due July 18. Appropriate files can be uploaded through the EasyChair website. The pre-proceedings version of the paper should be prepared for the LNCS format using Latex with the correct font type and size, borders, and spacing as indicated on the LNCS web site www.springer.com/lncs. Authors should use only outline fonts except for some special fonts otherwise unavailable and limit use of bitmaps for figures. The page limit for pre-proceedings papers is 20 pages, including bibliography, but excluding all appendices. Failure to abide by these rules may result in exclusion from the pre-proceedings and conference. If you feel an exception should be made in your case, contact the chairs as early as possible.

LNCS Proceedings: The LNCS proceedings will be published following the conference. More information on preparing the final LNCS proceedings version will be given after the conference. The page limit for the LNCS proceedings papers is still to be determined, but it will be under 20 pages, including all appendices. Therefore it is advisable to prepare your pre-proceedings version taking this into account.

Reviews: In preparing an update of their paper, authors must take into account reviewers' recommendations as much as possible. Papers with a number of serious reviewer comments that are not taken into consideration may face a late rejection. If you are concerned because you decide to not address some serious comments, send us an email at sac2016@mun.ca with an explanation so that we know that you have considered the comments.

Some other important items to keep in mind:
- All accepted papers must be presented by one of the paper's authors or the paper will be withdrawn from the conference and proceedings.
- At least one author of a paper should register by July 18. This also ensures a reduced registration fee.
- Book your flight as soon as possible to improve your chances of getting good fares and routes. When booking your flight, be sure to use airport code YYT for St. John's, Newfoundland.
- Consider coming to the SAC Summer School, Aug. 8-9 and encourage your colleagues to do so, as well!
- If you require a letter of invitation to obtain a visa to travel to Canada, let us know at sac2016@mun.ca right away since time is very tight. Links to information on visa requirements to Canada can be found on the SAC webpage.
- In the case that you are a visa-exempt foreign national, please check on the following web site of the Government of Canada to verify whether you need an Electronic Travel Authorization (eTA) to enter Canada www.cic.gc.ca/english/visit/eta.asp.
- The conference has a limited number of rooms reserved at the Sheraton Hotel, Quality Hotel, and the Memorial University residence. These rooms are only reserved up to July 10. So we

suggest booking your room as soon as possible. Visit the SAC webpage to see more.
- A limited number of seats are available for the puffin/whale watching tour. If you are interested, book early to ensure a spot and to receive a discount on the price.

Do not hesitate to contact us at sac2016@mun.ca if you have any questions.

We look forward to seeing you and/or your colleagues at SAC in St. John's!

Roberto Avanzi and Howard Heys

----------------------- REVIEW 1 ---------------------
PAPER: 104
TITLE: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
AUTHORS: Dustin Moody, Ray Perlner and Daniel Smith-Tone

----------- Review -----------
The authors show an attack faster than brute key search on the CubicABC multivariate encryption primitive.
Although the key recovery is still not within computing power for the proposed parameters, it shows that the
purported security has to be revised.
The attack uses invariant properties of low-dimensional subspaces of some tensor space. It is a variant of
MinRank.
Convincing work, deserving publication.

Minor remarks:
-p1: maleability -> malleability
-p2: define q in the introduction.
-p3: indeterminants -> indeterminates
-p4: definition 2: \bf a is in V_1, not V_2
-p5: bilnear -> bilinear

----------------------- REVIEW 2 ---------------------
PAPER: 104
TITLE: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
AUTHORS: Dustin Moody, Ray Perlner and Daniel Smith-Tone

----------- Review -----------
The paper extend the key recovery attack in [1] to the cubic ABC encryption scheme.
This attack is much more successful than applying the same technique to the quadratic ABC scheme. The expected operations to break 80-bit and 100-bit security parameters are 2^76 and 2^84 respectively.

The authors first searched for a subspace differential invariant of public keys. This column band-space were exploited by the it's low rank in differential form. The low rank distinguisher was further extended to full key recovery attack.

Strengths:
The authors point out the structure distinguisher of public key of ABC scheme from random systems.

Weaknesses:
The degradation in security due this attack is not astonishing comparing to direct algebraic attack.

Other comments: It was known folklorishly that rank-based attacks and subspace invariants work better for cubic multivariate schemes than for cubic ones, but this is the first time that someone noted this explicitly. It is also long known that there are various "gotchas" or flaws that when present help the efficiency of linear algebra based attacks in [2].

[1] Moody, Perlner and Smith-Tone: Any asymptotically optimal structural attack on the ABC multivariate encryption scheme. PQ Crypto 2014.

[2] Yang and J.-M. Chen: Building Secure Tame-Like Multivariate Public-Key Cryptosystems: the New TTS, ACISP 2005

----------------------- REVIEW 4 ---------------------
PAPER: 104
TITLE: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
AUTHORS: Dustin Moody, Ray Perlner and Daniel Smith-Tone

----------- Review -----------
The paper presents a key recover attack on the cubic ABC multivariate encryption scheme proposed in [13]. The original quadratic ABC scheme [11] was shown to be asymptotically insecure in [12], and the paper extends the techniques of [12], and applies them to the cubic

scheme. Technically (as in [12]), it exploits a differential invariant property of the core map to perform a key recovery attack. The attack is claimed to be more efficient than the estimated security of the scheme both in asymptotics as well as in practical parameters.

The paper is well-written and is of some interest. My main concern is that the techniques presented seem to be a straightforward adaptation of the ones of [12] (although I am not very familiar with [12]). I suggest that the authors clearly specify in a single place how their attack differs from the one of [12] (besides the definition of the subspace differential invariant over a cubic map).

It seems that the bit complexity of the attack may be underestimated, e.g., the linear algebra coefficient is taken to be 2.373, while ignoring the associated constant. This may be important, since the complexity of the attacks (especially the one on the 80-bit version) is quite close to the claimed complexity.

----------------------- REVIEW 5 ---------------------
PAPER: 104
TITLE: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
AUTHORS: Dustin Moody, Ray Perlner and Daniel Smith-Tone

----------- Review -----------
The manuscript describes a key recovery attack on the cubic ABC simple matrix multivariate encryption scheme introduced by Ding, Petzoldt and Wang at PQCrypto 2014. For the version of the scheme designed for 100-bit security, the attack breaks the scheme in approximately 2^84 operations. Experimental results are presented for the most costly step of the attack, which show a good agreement of experimental data with results predicted analytically.

----------------------- REVIEW 6 ---------------------
PAPER: 104
TITLE: Key Recovery Attack on the Cubic ABC Simple Matrix Multivariate Encryption Scheme
AUTHORS: Dustin Moody, Ray Perlner and Daniel Smith-Tone

----------- Review -----------
We kindly ask the authors to address the comment
"It seems that the bit complexity of the attack may be underestimated, e.g., the linear algebra coefficient is taken to be 2.373, while ignoring the associated constant. This may be important, since the complexity of the attacks (especially the one on the 80-bit version) is

quite close to the claimed complexity."

For instance, what happens if matrix multiplication complexity is not O(n^2.373) but instead O(n^3)?
This should be addressed at least in proper remarks.