From: Perlner, Ray (Fed)
To: (b) (6); Smith-Tone, Daniel (Fed)
Subject: RE: FW: Review Request
Date: Monday, March 13, 2017 4:07:00 PM

The primary result of the paper is a polynomial time reduction between two NP complete problems (the syndrome decoding problem and the MQ problem over GF2.) The paper showed how to solve a generic instance of the MQ problem by converting it to an instance of the syndrome decoding problem, via a tool which seems most suited to symmetric cryptanalysis, called the multiple right hand side (MRHS) representation.

The result appears to be correct, and the algorithm is interesting, however it is not so clear how significant the result is. The result is not very tight, since solving the MQ problem in the way indicated by the paper would be exponential in the square of the number of variables, n^2, whereas the trivial way of solving the MQ problem (guessing) is only exponential in n. It is also not surprising that such a reduction exists; indeed the fact that both problems are known to be NP complete indicates that such a reduction must exist. Finally, the instances of the MQ and syndrome-decoding problems typically used in cryptography are not generic, so it is unclear how much such reductions should add to our confidence in the security of actual cryptographic schemes.

Overall, the paper would be a respectable choice to publish, but may be rejected to make way for a more impactful result.

(weak reject)

From: Daniel Smith (b) (6)
Sent: Thursday, March 02, 2017 12:22 PM
To: Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: FW: Review Request

Thanks. Here is the paper.

On Thu, Mar 2, 2017 at 11:06 AM, Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov> wrote:

> **From:** Perlner, Ray (Fed)
> **Sent:** Thursday, March 2, 2017 11:06:34 AM (UTC-05:00) Eastern Time (US & Canada)
> **To:** Smith-Tone, Daniel (Fed)
> **Subject:** RE: Review Request
>
> Sure. Why not.
>
> Cheers,
> Ray
>
> **From:** Smith-Tone, Daniel (Fed)
> **Sent:** Thursday, March 02, 2017 4:34 AM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>

Subject: Review Request

Hi, Ray,

Would you be willing and available to review a paper for PQCRYPTO? The paper tries to build a connection between multivariate and code-based cryptosystems. They are trying to determine the complexity of solving MQ systems with decoding tools. If you are able, I would need the review by about the 20th to be able to input the review into the system by my deadline. Please let me know. Thanks.

Cheers,
Daniel