From: Kerman, Sara J. (Fed)
To: chad.boutin@nist.gov
Cc: Marron, Jeffrey A. (Fed); Smith, Lorin T. (Fed)
Subject: CSD Weekly WERB Update
Date: Thursday, December 12, 2019 10:06:00 PM

Hi Chad,
A couple papers started the WERB process this week:

Journal Paper Twisted Hessian Isogenies (PUB #929415)
Authors: **Moody, Dustin**; Dang, Thinh H. ;
International Journal of Number Theory

Abstract Elliptic curves are typically defined by Weierstrass equations. Given a kernel, the well-known V Velu's formula shows how to explicitly write down an isogeny between Weierstrass curves. However, it is not clear how to do the same on other forms of elliptic curves without isomorphisms mapping to and from the Weierstrass form. Previous papers have shown some isogeny formulas for (twisted) Edwards, Huff, and Montgomery forms of elliptic curves. Continuing this line of work, this paper derives an explicit formula for isogenies between elliptic curves in (twisted) Hessian form.

Conference Combinatorial Rank Attacks Against the Rectangular Simple Matrix Encryption Scheme (PUB #929413)
Authors: Moody, Dustin; Perlner, Ray A. ; Smith-Tone, Daniel C. ; Apon, Daniel C. ; Verbel, Javier;
PQCrypto 2020: The Eleventh International Conference on Post-Quantum Cryptography

Abstract In 2013, Tao et al. introduced the ABC Simple Matrix Scheme for Encryption, a multivariate public key encryption scheme. The scheme boasts great efficiency in encryption and decryption, though it suffers from very large public keys. It was quickly noted that the original proposal, utilizing square matrices, suffered from a very bad decryption failure rate. As a consequence, the designers later published updated parameters, replacing the square matrices with rectangular matrices and setting parameters to avoid the cryptanalysis of the original scheme presented in 2014 by Moody et al. In this work we show that making the matrices rectangular, while decreasing the decryption failure rate, actually, and ironically, diminishes security. We show that the combinatorial rank methods employed in the original attack of Moody et al. can be enhanced by the same added degrees of freedom that reduce the decryption failure rate. Moreover, and quite interestingly, if the decryption failure rate is still reasonably high, as exhibited by the proposed parameters, we are able to mount a reaction attack to further enhance the combinatorial rank methods. To our knowledge this is the first instance of a reaction attack creating a significant advantage in this context.

Sara J. Kerman
NIST/ITL/Division 773

Bldg. 222, Room B347
X4634