

**From:** [Kerman, Sara J. \(Fed\)](#)  
**To:** (b) (6)  
**Cc:** [Perlner, Ray A. \(Fed\)](#); [Smith-Tone, Daniel C. \(Fed\)](#)  
**Subject:** RE: Copy of "HFERP -- A New Multivariate Encryption Scheme"  
**Date:** Wednesday, January 24, 2018 10:17:38 AM

---

Thanks Daniel!

**From:** Daniel Smith (b) (6)  
**Sent:** Wednesday, January 24, 2018 10:14 AM  
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>  
**Cc:** Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>  
**Subject:** Re: Copy of "HFERP -- A New Multivariate Encryption Scheme"

Hi, Sara,

Here is a copy! Thanks!

Cheers,  
Daniel

On Wed, Jan 24, 2018 at 10:12 AM, Kerman, Sara J. (Fed) <[sara.kerman@nist.gov](mailto:sara.kerman@nist.gov)> wrote:

Ray,

I can't move forward with WERB approvals of your 1<sup>st</sup> PQCrypto 2018 submission without a copy of the paper for reviewers to read. Please send me a copy since it was not attached to the NIKE/WERB record.

Thanks,  
Sara

---

**From:** Kerman, Sara J. (Fed)  
**Sent:** Tuesday, January 23, 2018 9:37 AM  
**To:** Perlner, Ray (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Cc:** Smith-Tone, Daniel (Fed) <[daniel.smith@nist.gov](mailto:daniel.smith@nist.gov)>; (b) (6)  
(b) (6)  
**Subject:** WERB Request Entered

Ray,

Can you please send me an electronic version of this paper? "HFERP -- A New Multivariate Encryption Scheme"

---

**From:** Kerman, Sara J. (Fed)  
**Sent:** Wednesday, January 17, 2018 9:09 AM  
**To:** Perlner, Ray (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Cc:** Smith-Tone, Daniel (Fed) <[daniel.smith@nist.gov](mailto:daniel.smith@nist.gov)>; (b) (6)

(b) (6)

**Subject:** FW: Publication Request Entered

Hey Ray,

The paper didn't get attached to the NIKE record. Can you forward to me and I'll upload?

Thanks,

Sara

**From:** ITL Publication Database [[mailto:nike\\_isg@nist.gov](mailto:nike_isg@nist.gov)]

**Sent:** Wednesday, January 17, 2018 8:31 AM

**To:** Honeycutt, Diane (Fed) <[diane.honeycutt@nist.gov](mailto:diane.honeycutt@nist.gov)>

**Subject:** Publication Request Entered

A publication request was entered, as the secretary for the group, please go to the Publication Database and click "Check Manuscript Requests"

URL: <https://nike.nist.gov/publications/checkManu.do>

Publication title: HFERP -- A New Multivariate Encryption Scheme

Publication ID: 925152

ERB Control #: Not Assigned

Laboratory: 77 - Information Technology Laboratory

Division: 773 - Computer Security Division

Performing Organization: Gaithersburg

Authors:

\* Author 1: Perlner, Ray; 773.01; [ray.perlner@nist.gov](mailto:ray.perlner@nist.gov); (301) 975-3357 Mailstop 8930

Author 2: Smith-Tone, Daniel; 773.01; [daniel.smith@nist.gov](mailto:daniel.smith@nist.gov); (301) 975-3870

Author 3: Ikematsu, Yashuhiko; Kyushu University; JP;

Author 4: Takagi, Tsuyoshi; Kyushu University; JP;

Author 5: Vates, Jeremy; University of Louisville; 40292; KY; US;

\* - Point of Contact

Proposed Publication:

Conference: PQCrypto 2018: The Ninth International Conference on Post-Quantum Cryptography  
Fort Lauderdale, FL, United States, 04/09/2018 to 04/11/2018

Publication Location: US

Division Reader: Moody, Dustin

ERB Reader: Liu, Yi-Kai

ERB Reader Division: 771