Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan
iwata@cse.nagoya-u.ac.jp

January 14, 2012

To whom it may concern,

I would like to submit brief comments on EAXprime (EAX'). We have investigated its cryptographic strength as a general purpose authenticated encryption, and the report is now available at http://eprint.iacr.org/2012/018.

Our report shows simple and efficient forgery and distinguishing attacks on EAXprime. Our attacks require specific format and length on its input, and we do not know if our attacks can be extended to the protocol that strictly follows the ANSI C12.22 specification. However, our results indicate that the security of EAXprime cannot be proved, and that EAXprime is cryptographically broken as a general purpose authenticated encryption. Therefore, EAXprime does not offer the same security level as other provably secure authenticated encryptions, including the original EAX.

Given the attacks, I believe that EAXprime is not an appropriate mode to be included in the 800-38 series of NIST Special Publications as a general purpose authenticated encryption.

Sincerely,

Tetsu Iwata