From: D. J. Bernstein [djb@cr.yp.to]
Sent: Friday, July 17, 2009 6:54 AM
To: hash-function@nist.gov
Cc: hash-forum@nist.gov
Subject: OFFICIAL COMMENT: FSB

I'm coauthor of a paper "FSBday: Implementing Wagner's generalized birthday attack against the SHA-3 candidate FSB" with Tanja Lange, Ruben Niederhagen, Christiane Peters, and Peter Schwabe. The paper has been accepted for presentation at SHARCS 2009 and can be found online at http://eprint.iacr.org/2009/292.

Our implementation is state-of-the-art; it combines several old and new improvements. Our paper nevertheless concludes that the FSB compression function is oversized. The FSB designers used an extremely conservative lower bound for the cost of Wagner's attack (and other attacks), and chose parameters to be safe against that lower bound; a more precise analysis shows that considerably smaller parameters are secure.

Peter Schwabe has also contributed to eBASH a new implementation of
FSB-256 (with the originally specified parameters), using only 92 cycles/byte on a single core of a Core 2 Quad Q9550 (10677, berlekamp).
Tuning of the load patterns in the implementation is likely to produce further speedups across a wide variety of platforms.

---D. J. Bernstein
Research Professor, Computer Science, University of Illinois at Chicago