From: hash-forum@nist.gov on behalf of Sean O'Neil [s.oneil@vest.fr]
Sent: Wednesday, July 01, 2009 3:12 PM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: EnRUPT

After a long analysis and due consideration, we have decided to propose EnRUPT/8 for all three 64-bit variants: EnRUPT64x2-256/8,
EnRUPT64x2-384/8 and EnRUPT64x2-512/8 as our updated SHA-3 submission.

In simple terms, the same security parameter s=8 is chosen for different sizes due to the fact that the most effective [linearized collision] attacks cannot break a greater number of rounds for the larger sizes with their much higher security levels that allow for much more expensive attacks. Since more expensive attacks cannot break a greater number of rounds, the attacker’s control is limited equally for all the different sizes, most probably by the word width equally limiting the attacker’s control. Therefore, an equal number of rounds is sufficient for the different sizes, while the higher security is achieved by increasing the size of the state. Although we firmly believe in the cryptographic resistance of s>=5 and we are working on a proof of its resistance to linearization attacks, we propose s=8 to establish a sufficient margin from the best known attacks (2x) to ensure a lasting public trust in the algorithm.

The latest improved 64-bit C and the new Intel Assembly implementations also bring the speed of EnRUPT/8 from 10 to 7.8 CPB (Core 2 Duo, with minor variations on different CPUs) placing it somewhere between Tiger and SHA-1.

We will publish and submit the updated specification including the updated optimized implementation soon.

With best regards,
The EnRUPT Team