

Subject: OFFICIAL COMMENT: ECHO

From: "Thomas PEYRIN" <Thomas.PEYRIN@ingenico.com>

Date: Wed, 4 Feb 2009 09:56:21 +0100

To: <hash-function@nist.gov>

Hi all,

We have updated our implementations of ECHO, the new assembly code will soon be available at the following webpage: <http://crypto.rd.francetelecom.com/echo/>

On the NIST platform, we now have the following speed results:

ECHO-256

64-bit mode: 28,5 c/B

32-bit mode: 32,5 c/B

ECHO-512

64-bit mode: 53,5 c/B

32-bit mode: 61 c/B

Cheers,

The Echo Team.

About Ingenico: Ingenico is the world's leading provider of payment solutions, with over 15 million te deployed across the globe. Delivering the very latest secure electronic payment technologies, transaction management and the widest range of value added services, Ingenico is shaping the future direction of the payment solutions mar Leveraging on its global presence and local expertise, Ingenico is reinforcing its leadership by taking banks and businesses beyond payment through offering comprehensive solutions, a true source of differentiation and new revenues streams.

This message may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message. Thank you for your cooperation.

P Please consider the environment before printing this e-mail