From: "Brian Gladman" <brian.gladman@btinternet.com>
To: "Elaine Barker" <elaine.barker@nist.gov>, "Jim Foti" <jfoti@nist.gov>
Cc: "Tudor Brown" <tudor.brown@arm.com>
Subject: £rd AES Conference Paper
Date: Sun, 16 Jan 2000 20:51:12 -0000
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

Hi Jim, Elaine

I am able to offer a written paper for the 3rd AES Conference but since the work is not yet complete I can only offer an abstract at this stage. This is as follows:

AES Implementation Experience on the ARM Architecture

There is considerable evidence of the performance of the AES candidate algorithms on high end machines but less is known about their performance on embedded processors. This is problematic because many future applications of encryption will use embedded processors.

The paper will look at the implementation of the five second round candidates on the ARM architecture. This architecture offers a useful test of the AES algorithms in respect of implementation performance because it is available in a range of different processor configurations. At the low end these are capable of operating on smartcards and in embedded systems whilst high end performance is also available using the StrongARM processor. In addition, since ARM employs a RISC philosophy, the paper will also provide evidence of AES algorithm performance of machines of this character.

The paper will present implementation experience and performance results for the five AES finalists on the ARM architecture when coded in both C and in assembler. It will draw conclusions about the relative implementation complexity of these algorithms by considering the time cost of assembler implemtation and the ratio of C to assembler code performance.

It is uncertain whether I will be able to secure the sponsorship I would need to present the paper at the Conference.

Status or work:

1. All five algorithms evaluated in C on ARM

2. Three of five completed in assembler, one part completed, one remaining.

I am hence confident that I can complete the work in time for the Conference in April.

Please note that this work has been part sponsored by ARM Limited who have kindly provided development support for the effort.

best regards, Dr Brian Gladman, Worcester UK, 16th January 2000