X-Sender: kanda@sucaba.isl.ntt.co.jp
X-Mailer: QUALCOMM Windows Eudora Pro Version 3.0.3-J (32)
Date: Thu, 15 Apr 1999 21:47:28 +0900
To: AESFirstRound@nist.gov
From: Masayuki KANDA <kanda@sucaba.isl.ntt.co.jp>
Subject: Official comment
Cc: kanda@sucaba.isl.ntt.co.jp

Dear sirs,

I send an official comment for AES develop effort on
"Comments on Hardware Implementation of E2."
(Filename: comment_hard.ps)

Please check my paper, and if you cannot read the paper,
contact me immediately.

Contact to:
Masayuki Kanda
E-mail: kanda@sucaba.isl.ntt.co.jp
Tel: +81 468 59 2437
Fax: + 81 468 59 3858
Affiliate: NTT Laboratories
Address: 1-1-612A Hikarinooka, Yokosuka-shi, Kanagawa,
239-0847, Japan

Thank you in advance.

Best regards,

##
NTT Information Sharing Platform Laboratories - Security Project
(Notice: Names of NTT's Laboratories are altered after 25 Jan. 1999)

Masayuki Kanda
E-Mail : kanda@sucaba.isl.ntt.co.jp
Postal : 1-1-612A Hikarinooka Yokosuka-shi Kanagawa 239-0847 Japan
FAX : +81 468 59 3858 Phone : +81 468 59 2437 (Dial in)

Comments on Hardware Implementation of *E2*

Nippon Telegraph and Telephone Corporation (NTT)*

April 15, 1999

Abstract

This paper shows the latest estimation of the dedicated LSI components of ***E2***. Since ***E2*** has many possible space-time tradeoffs, we built three components with different sizes of the data randomizing part and the key scheduling part. As a result, we believe that ***E2*** is one of the fastest ciphers and is no larger in size than most other AES candidates.

1 Our estimation

Our estimations are all based on the design compiler made by Synopsys Inc. and the 0.25 micron rule CMOS cell based library made by NTT Electronics. Since ***E2*** uses familiar primitive operations, we can use standard cells for each operation, including 32×32 integer multiplication.

Roughly speaking, our LSI component consists of three areas: key scheduling area *including registers for all subkeys*, data randomizing area, and the other area such as data buffers. Most components lie in the key scheduling area and data randomizing area.

Note that, since the encryption and decryption processes of ***E2*** are identical, the decryption process including subkey generation does not require any penalty in throughput, area, or subkey generation time. In some AES candidates, e.g., Rijndael, RC6, Serpent, Mars, etc., decryption is not entirely identical to encryption. This means that component size is roughly doubled to execute decryption. Accordingly, for fair hardware comparison, the estimations should clarify the environment and limitation of the components; e.g., whether they include subkey registers or not, whether they can use decryption or not, etc.

*Contact to: kanda@sucaba.isl.ntt.co.jp

2 Latest estimation of our dedicated LSI components

Table 1 shows, for ***E2***, the current hardware throughput for any secret key length (128-, 192-, 256-bit) with several speed-area tradeoffs. In this paper, all estimations are for typical cases. "Gate" means a 2-input NAND gate, equivalent to 4 transistors.

Type 1 was shown at the 1st AES conference and described in our supporting document (please see also errata on E2 home page[1]). It is the fastest version, while its area is largest. It is fully parallelized; i.e., it has sixteen logical s-boxes and four 32×32-bit multipliers in the data randomizing part, and two f-functions, two 32×32-bit multipliers in the key scheduling part. It takes 1 cycle to complete each F-Function, IT/FT-Functions, and plain/cipher text load/store. Thus, it can produce the throughput of one block every 16 cycles, or 1 Gbits/sec at 125 MHz. The key scheduling part computes an inverse element for FT-Function using the Zassenhaus algorithm.

Type 2 reduces the key scheduling area. It is also fully parallelized in the the data randomizing part; i.e., it has sixteen s-boxes (ROM), and four 32×32-bit multipliers. Similar to type 1, it takes 1 cycle to complete each F-Function, IT/FT-Functions, and plain/cipher text load/store. Thus, it can produce the throughput of one block every 16 cycles, or 912 Mbits/sec at 114 MHz. On the other hand, the key scheduling part is serialized; i.e., it has only one 32-bit adder instead of two multipliers, and one f-function. The key scheduling area is almost one third of that of type 1, but has a large penalty in generating subkeys more slowly, almost 30 times

[1] http://info.isl.ntt.co.jp/e2/

Table 1: Hardware throughput

		Type1	Type2	Type3
Key scheduling	(Kgates)	65.4	23.3	23.3
Data randomizing	(Kgates)	61.5	45.6	38.2
Total	(Kgates)	140	82	74.6
Key setup	(clocks)	56	772	772
	(nsec/key)	504	15440	15440
clock rate	(MHz)	111	50	50
Encryption/Decryption	(clocks)	16	16	18
	(Mbits/sec)	1000	912	818
clock rate	(MHz)	125	114	115

slower. The key scheduling part computes an inverse element for FT-Function using the Hensel lifting for modular inverse algorithm. Type 2 is useful for encrypting large data with the same key.

Type 3 is another reduced version. It reduces the area of the data randomizing part; i.e., it has sixteen s-boxes (ROM), and two 32×32-bit multipliers, while it has the same key scheduling part as type 2. Since it takes 1 cycle to complete each F-Function and data load/store, and 2 cycles to complete IT/FT-Functions, it can produce the throughput of one block every 18 cycles, or 818 Mbits/sec at 115 MHz.

As mentioned above, ***E2*** has many possible space-time tradeoffs in hardware implementation. For example, we can also consider a smaller version that has eight s-boxes (ROM), and one 32×32-bit multiplier. We expect it to have approximately 25 Kgates in the data randomizing part, which takes almost 50 clocks or 384 Mbits/sec at 150 MHz.

Once again, since the encryption and decryption processes of ***E2*** are exactly identical, the decryption process including subkey generation does not require any penalty in throughput, area, and subkey generation time. Thus, we believe that ***E2*** is one of the fastest ciphers and is no larger in size than most other AES candidates, though Schneier et al. mentioned that ***E2*** is large in hardware in [2].

3 Related paper

Ichikawa et al. showed preliminary hardware estimations of some block ciphers including four AES candidates: ***E2***, Mars, RC6, Serpent, and DES, Triple-DES [1] at SCIS'99 in Kobe, Japan. Their estimation is based on the design compiler made by Synopsys Inc. and the 0.35 micron rule CMOS cell based library made by Mitsubishi Electronics. They showed that the critical-path of ***E2*** is 225.16 nsec, which is close to those of Triple-DES and Serpent, and so is 3 times faster than RC6 and Mars. In other words, the typical throughput of one block of ***E2*** is approximately 1 Gbits/sec, which is similar to our result, without pipelining.

References

[1] T. Ichikawa, T. Kasuya, and M. Matsui, "On Hardware Implementation of 128-bit Block Ciphers (I)," *the 1999 Symposium on Cryptography and Information Security SCIS'99*, F1-2.3, pp. 807–812, 1999. (in Japanese).

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions," *The second AES conference*, pp. 1–20, 1999.