From: maro@isl.ntt.co.jp
To: AESFirstRound@nist.gov
Subject: Software Implementation Results of E2
Date: Fri, 16 Apr 1999 00:29:33 JST
Sender: maro@sucaba.isl.ntt.co.jp

Dear Director/ITL,

I submit the report titled
  Software Implementation Results of E2
using PostScript. The file is generated with gzip and
uuencode. If you cannot print the file, please ask me.

Best regards,

/ NTT Laboratories
/ AOKI, Kazumaro
/ E-mail: maro@isl.ntt.co.jp

Software Implementation Results of *E2*

Kazumaro Aoki* and Hiroki Ueda†
NTT Laboratories‡

April 15, 1999

1 Implementations on 32- and 64-bit Processors

We updated the software implementation results of ***E2*** [N98a, N98b] using new optimization techniques [AU99]. Table 1 shows the current best results on 32- and 64-bit processors.

Note that as follows:

- The throughput of decryption is the same as that of encryption, since the encryption process and decryption process are identical except for the order of subkeys.
- The impact of NIST API overhead can be considered as small, because we encrypted (decrypted) large data blocks.
- The reason for the dependency of key scheduling time on key length is that we precomputed the values for padding.

At the Second Advanced Encryption Standard Conference (AES2), NIST presented the results of software efficiency tests on each AES candidate [U99]. Since the results included the speeds of small block encryption and large block encryption, we tested our codes using similar scenarios as shown in Table 2. Here, the speed measurements include many overheads; e.g., loop overhead, memory fetch and store operations (for encryption/decryption data), endian conversions, etc. Table 2 shows the averaged clocks per one block encryption or decryption. Note that our measurements are performed on Pentium Pro and Pentium II with 8KB and 16KB of the first level cache, and 256KB and 512KB of the second level cache, respectively.

2 Implementations on Smart Card

E2 can be efficiently implemented on from mid- to high-end smart cards. We implemented ***E2*** on H8/300[1] as an example of a mid-end smart card, and Hachez et al. implemented ***E2*** on ARM as an example of a high-end smart card [HKQ99].

Schneier et al. [SKW+99, Section 5.2.5 in p.26(p.12)] and Hachez et al. [HKQ99, Section 5.1.1 in p.100(p.6)] described that ***E2*** implementation requires at least 256 bytes of RAM. However, ***E2*** can be implemented on even low-end smart cards. Actually, we have implemented ***E2*** on a 8052 whose RAM size is 256 bytes; this version takes about 34000 cycles. To implement ***E2*** on such low-memory smart cards, our implementation calls the key-setup

*Email: maro@isl.ntt.co.jp
†Email: ueda@isl.ntt.co.jp
‡1-1 Hikarinooka, Yokosuka-shi, Kanagawa-ken, 239-0847 Japan
[1]Its specification is similar to Motorola 68x.

Table 1: ***E2*** Software Performance on 32- and 64-bit Processors

CPU	Language	Key length (bit)	En(De)cryption (clks/blk)	(bits/s)	Key scheduling[a] (clks/key)
Pentium Pro[b]	ANSI C[c]	128	655	39.1M	2076
		192	655	39.1M	2291
		256	655	39.1M	2484
	VC++[d]	128	584	43.8M	1868
		192	584	43.8M	2042
		256	584	43.8M	2278
	Assembly	128/192/256	375	68.3M	
	Java[e]	128/192/256	2370	10.8M	
	Java[f]	128/192/256	28800	0.9M	
Pentium II[g]	ANSI C[c]	128/192/256	630	91.4M	
	VC++[d]	128	561	102.7M	1804
		192	561	102.7M	1991
		256	561	102.7M	2228
	Assembly	128/192/256	355	162.3M	
Alpha[h]	Assembly	128/192/256	587	130.8M	

[a]Clocks of key scheduling do not include NIST API overhead.
[b]NIST AES Analysis Platform; IBM compatible PC, Pentium Pro (200MHz), MS-Windows95, 64MB RAM
[c]Borland C++ 5.02
[d]Microsoft Visual C++ 5.0 Enterprise Edition
[e]JDK 1.1.6 with JIT compiler
[f]JDK 1.1.6 without JIT compiler
[g]IBM compatible PC, Pentium II (450MHz), MS-Windows95, 256MB RAM
[h]DEC Alpha 21164A (600MHz), Digital Unix 4.0, 8MB 3rd cache, 256MB main memory

Table 2: ***E2*** Speed Variations on Pentium Pro/II

Language	Data length (bytes)	(blocks)	En(De)cryption Pentium Pro[a] (clks/block)	Pentium II[b] (clks/block)
ANSI C[c]	1K	64	654	629
	128K	8K	676	649
	1M	64M	680	684
VC++[d]	1K	64	586	563
	128K	8K	601	581
	1M	64M	612	616
Assembly	1K	64	375	355
	128K	8K	386	374
	1M	64M	397	404

[a]NIST AES Analysis Platform; IBM compatible PC, Pentium Pro (200MHz), MS-Windows95, 64MB RAM
[b]IBM compatible PC, Pentium II (450MHz), MS-Windows95, 256MB RAM
[c]Borland C++ 5.02
[d]Microsoft Visual C++ 5.0 Enterprise Edition

routine several times during each encryption or decryption. We believe that this technique is useful in implementing ***E2*** on any low-end smart card. See [AU99, Appendix] for more details.

These results are summarized in Table 3 for the case of a 128-bit key.

Table 3: Smart Card Performance of ***E2***

CPU	RAM usage (bytes)	ROM usage (bytes)	Key scheduling		Encryption	
8051[a]	105[b]	1284[c]	100092cycles	(100ms)		
8052[d]	210	1300	34000cycles	(34ms)		
H8/300[e]	686	12929[f]	14041cycles	(2.81ms)	6370cycles	(1.27ms)
	420	4292[f]	22422cycles	(4.48ms)	7468cycles	(1.49ms)
8051[g]	344[h]	1444	26147cycles	(44ms)	9725cycles	(16ms)
ARM[i]	336	1260	8172cycles	(0.286ms)	2180cycles	(0.076ms)

[a] running at 12MHz (1 cycle = 12 oscillator periods). This result is very preliminary. The cycles of key scheduling and encryption will be significantly improved.

[b] including plaintext, master key, and stack areas.

[c] including tables.

[d] running at 12MHz (1 cycle = 12 oscillator periods). This result is an estimation based on 8051 results.

[e] running at 5MHz (1 cycle = 1 oscillator period).

[f] This result seems very large because the implementation is optimized for speed.

[g] running at 3.57MHz (1 cycle = 6 oscillator periods). [HKQ99]

[h] using external RAM.

[i] running at 28.56MHz (1 cycle = 1 oscillator period). [HKQ99]

References

[AU99] K. Aoki and H. Ueda. Optimized Software Implementations of E2. (`http://info.isl.ntt.co.jp/e2/`), 1999.

[HKQ99] G. Hachez, F. Koeune, and J.-J. Quisquater. cAESar results: Implementation of Four AES Candidates on Two Smart Cards. In *Second Advanced Encryption Standard Candidate Conference*, pp. 95–108, Hotel Quirinale, Rome, Italy, 1999. Information Technology Laboratory, National Institute of Standards and Technology.

[N98a] Nippon Telegraph and Telephone Corporation. *Specification of **E2** — a 128-bit Block Cipher*, 1998. (`http://info.isl.ntt.co.jp/e2/`).

[N98b] Nippon Telegraph and Telephone Corporation. *Supporting Document on **E2***, 1998. (`http://info.isl.ntt.co.jp/e2/`).

[SKW+99] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson. Performance Comparison of the AES Submissions. In *Second Advanced Encryption Standard Candidate Conference*, pp. 15–34, Hotel Quirinale, Rome, Italy, 1999. Information Technology Laboratory, National Institute of Standards and Technology.

[U99] U.S. Department of Commerce, National Institute of Standards and Technology. *NIST's Efficiency Testing for Round1 AES Candidates*, 1999. (`http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm`).