HITACHI

Hitachi, Ltd., Software, Division
5030, Totsuka-cho, Totsuka-ku
Yokohama, 244-8555 Japan
Tel: x-81-45-881-7161 Fax: x-81-45-865-9010

April 10, 2000

Mr. J. Terry Lynch
Information Technology Laboratory
Attn: AES Finalist Comments (Bilg. 820, Room 423)
100 Bureau Drive, STOP 8930
Gaithersburg, MD 20899-8930
U.S.A.

Dear J. Terry Lynch:

Thank you for your reply to our notification with respect to Hitachi, Ltd. U.S. patents related to AES candidates.

I would like to send required information to you.

(1) The U.S. patent numbers; USP4,982,429 USP5,103,479
Japanese patent numbers; 2,760,799 2,798,086 2,798,087 2,870,531 2,870,532 2,980,085 and several applications of Japanese patents.

(2) The abstracts of related U.S. patents: please refer to attached image files(US4982429.tif, US5103479.tif).

(3) Our view of the relationship between our patented technology and AES candidates is as follows: we think that four AES candidates (MARS, RC6, Twofish, Serpent) use encipher (decipher) methods which include several encipherment processes(or processes generating authentification-code) with different circular shifting bits.

We would like to show you some claim examples regarding to the above points:

USP5,103,479 claims:

“Claim1. An enciphering method for converting a pair of plain text data into a pair of ciphertext data by sequentially performing a plurality of encipherment processes on said pair of plaintext data, each of encipherment processes having a function to restore a pair of ciphered text data to a pair of former text data if each of said encipherment processes is performed again on said pair of ciphered text data, comprising the steps of: performing a first encipherment process for deriving a first pair of data from said pair of plain text data; performing a second encipherment process for deriving a second pair of data from said first pair of data by circular shifting of first intermediate data derived from one of said first pair of data by a first predetermined number of bits; performing a third encipherment process for deriving a third pair of data from said second pair of data by

circular shifting of second intermediate data derived from one of said second pair of data by a second predetermined number of bits which are different from said first predetermined number of bits; and performing a fourth encipherment process or other encipherment processes by deriving said pair of ciphertext data from said third pair of data."

"Claim 10. A method for generating code data by executing a plurality of arithmetical processes on message data, comprising the steps of: performing a first process for generating first intermediate data by arithmetically operating on second intermediate data derived from initial data having a predetermined bit pattern and a first portion of said message data; performing a second process for generating third intermediate data by circular shifting of said first intermediate data by a first predetermined number of bits; performing a third process for generating fourth intermediate data by arithmetically operating on fifth intermediate data derived from said third intermediate data and a second portion of said message data; performing a fourth process for generating sixth intermediate data by circular shifting of said fourth intermediate data by a second predetermined number of bits which is different from said first predetermined number of bits; performing a fifth process for generating seventh intermediate data by arithmetically operating on said sixth intermediate data and a third portion of said message data; performing a sixth process for generating eighth intermediate data by circular shifting of said seventh intermediate data by a third predetermined number of bits which is different from said second predetermined number of bits and by arithmetically operating on said eighth intermediate data, said seventh intermediate data, and said fourth intermediate data; and performing a seventh process for generating said code data by arithmetically operating on said eighth intermediate data."

Sincerely,

Shinichiro Harano
Shinichiro Harano

Director
IPR & Cryptographic Technology
Network Software
Software Divison
Hitachi, Ltd.