暗号技術仕様書　MISTY1

（updated 2002年5月13日）

2001年9月27日

三菱電機株式会社

ブロック暗号アルゴリズム MISTY1

本ドキュメントは、ブロック暗号アルゴリズム MISTY1 について記述したものである。MISTY1 は、128 ビットの暗号化鍵を持つ 64 ビットブロック暗号であり、段数nは可変(但し、nは 4 の倍数)とする。推奨値は n=8 である。なお、以下の記述や図に関しては、左側を最上位（MSB）とし、右側を最下位（LSB）と定義する。

データランダマイズ部

- 図 1a は MISTY1 の暗号化処理のデータランダマイズ部、図 1b は MISTY1 の復号処理のデータランダマイズ部をそれぞれ記述したものである。平文／暗号文 64 ビットは 32 ビット毎２つに分割され、排他的論理和⊕と副関数 $FO_i(1 \le i \le n)$、$FL_i(1 \le i \le n+2)$、$FL_i^{-1}(1 \le i \le n+2)$ によって変換を行う。FO_i では 64 ビットの拡大鍵 KO_i と 48 ビットの拡大鍵 KI_i が使用される。FL_i は暗号化に、また FL_i^{-1} は復号に用いられ、それぞれ 32 ビットの拡大鍵 KL_i が使用される。
- 図 2 は関数 FO_i を記述したものである。入力 32 ビットは 16 ビット毎２つに分割され、排他的論理和⊕と副関数 $FI_{ij}(1 \le j \le 3)$ によって変換を行う。$KO_{ij}(1 \le j \le 4)$ と $KI_{ij}(1 \le j \le 3)$ は、それぞれ KO_i と KI_i の左から j 番目の 16 ビットデータを使用する。
- 図 3 は関数 FI_i を記述したものである。入力 16 ビットは左 9 ビットと右 7 ビットのデータに分割され、排他的論理和⊕と置換表 S_7、S_9 によって変換を行う。1 番目と 3 番目の排他的論理和では、7 ビットデータを上位 2 ビットにゼロを付加して 9 ビットデータとして演算を行い(zero-extended)、2 番目の排他的論理和では、9 ビットデータの上位 2 ビットを切り捨てて 7 ビットデータとして演算を行う(truncated)。KI_{ij} の左 7 ビットデータを KI_{ij1} とし、右 9 ビットデータを KI_{ij2} とする。
- 図 4a ならびに図 4b は関数 FL_i および FL_i^{-1} を記述したものである。入力 32 ビットは 16 ビット毎２つに分割され、排他的論理和⊕と論理積 ∩、論理和 ∪によって変換を行う。$KL_{ij}(1 \le j \le 2)$ は、KL_i の左から j 番目の 16 ビットデータを使用する。
- 表 1、表 2 は置換表 S_7、S_9 を十進表現で表したものである。例えば表１は、S_7 に０を入力した時の出力が 27，1 を入力した時の出力は 50，2 を入力した時の出力は 51 等々を意味している。

鍵スケジュール部

- 図 5 は MISTY1 の鍵スケジュール部を記述したものである。秘密鍵 K の左から i 番目の 16 ビットデータをそれぞれ $K_i(1 \le i \le 8)$ とする。FI_{ij} の入力を K_i とし、KI_{ij} を K_{i+1} とした FI_{ij} の出力を $K_i'(1 \le i \le 8)$ とする。なお、K_9 は K_1 と同じものを表している。
- KO_{ij}、KI_{ij}、KL_{ij} と実際の鍵との関係は以下の表のようになっている。なお、i が８をこえる場合には、K_i と K_i' はそれぞれ K_{i-8} と K_{i-8}' を意味すると約束する。

	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{i1}	KL_{i2}
Key	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{\frac{i+1}{2}}$ (*odd i*) $K'_{\frac{i}{2}+2}$ (*even i*)	$K'_{\frac{i+1}{2}+6}$ (*odd i*) $K_{\frac{i}{2}+4}$ (*even i*)

テストデータ

- ８段の MISTY1 のサンプルデータを１６進表現で以下に記述する。

秘密鍵$(K_1 \cdots K_8)$	00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
平文	01 23 45 67 89 ab cd ef
拡大鍵$(K_1' \cdots K_8')$	cf 51 8e 7f 5e 29 67 3a cd bc 07 d6 bf 35 5e 11
暗号文	8b 1d a5 f5 6a b3 d0 7c

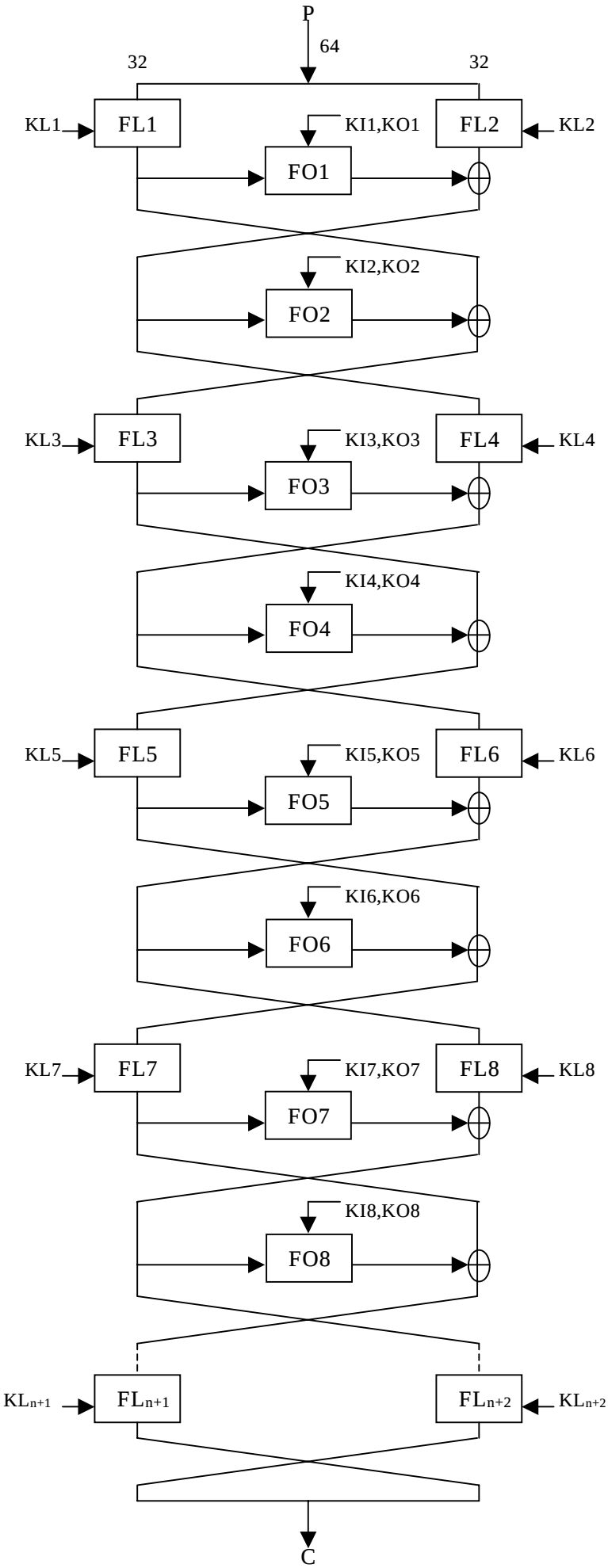


図 1a. MISTY1 暗号化

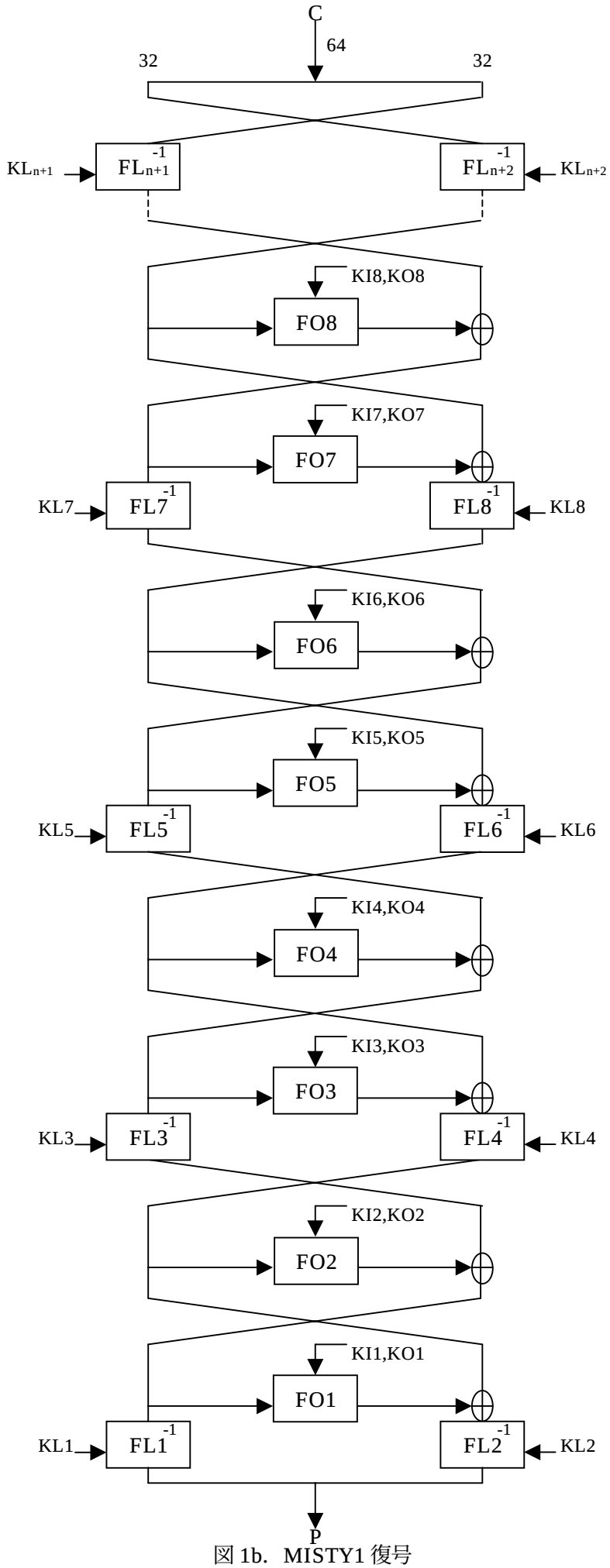


図 1b. MISTY1 復号

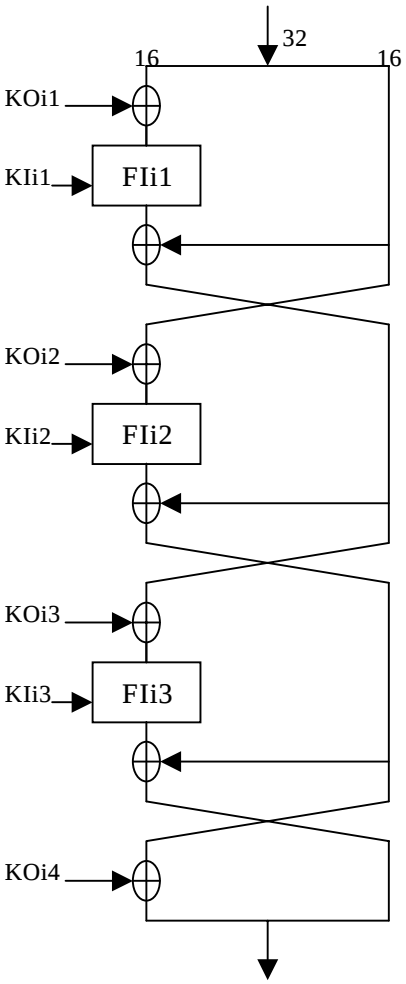


図 2. FOi

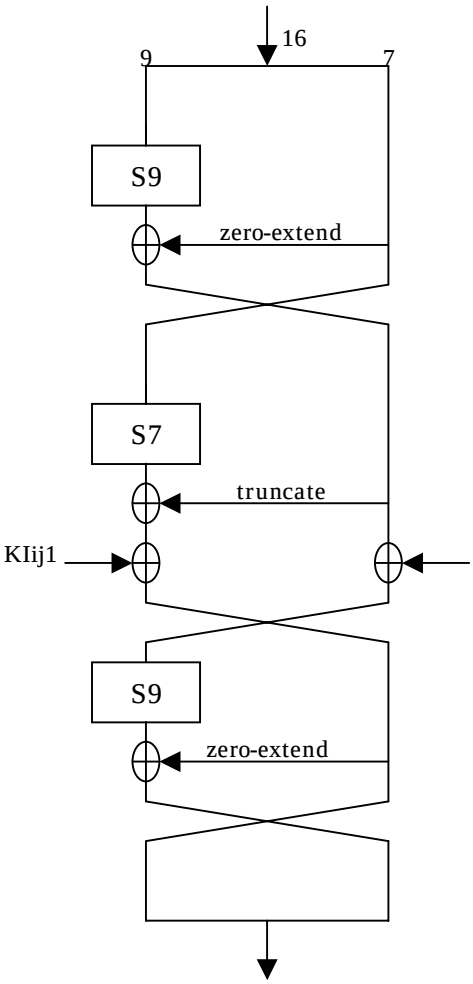


図 3. FIij

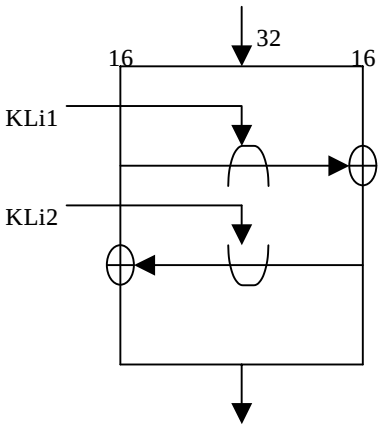


図 4a. FLi

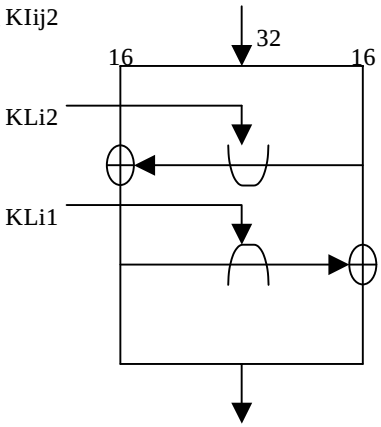


図 4b. FL i^{-1}

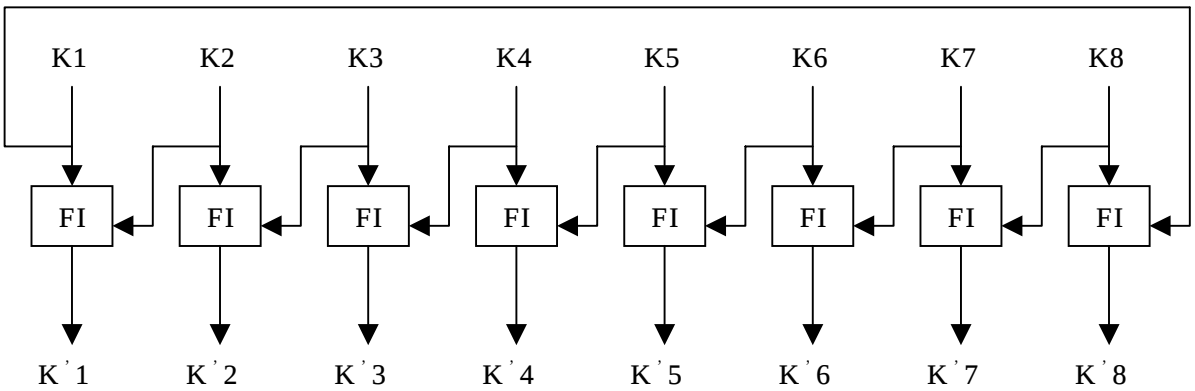


図 5. Key Scheduling

27, 50, 51, 90, 59, 16, 23, 84, 91, 26,114,115,107, 44,102, 73,
31, 36, 19,108, 55, 46, 63, 74, 93, 15, 64, 86, 37, 81, 28, 4,
11, 70, 32, 13,123, 53, 68, 66, 43, 30, 65, 20, 75,121, 21,111,
14, 85, 9, 54,116, 12,103, 83, 40, 10,126, 56, 2, 7, 96, 41,
25, 18,101, 47, 48, 57, 8,104, 95,120, 42, 76,100, 69,117, 61,
89, 72, 3, 87,124, 79, 98, 60, 29, 33, 94, 39,106,112, 77, 58,
 1,109,110, 99, 24,119, 35, 5, 38,118, 0, 49, 45,122,127, 97,
80, 34, 17, 6, 71, 22, 82, 78,113, 62,105, 67, 52, 92, 88,125

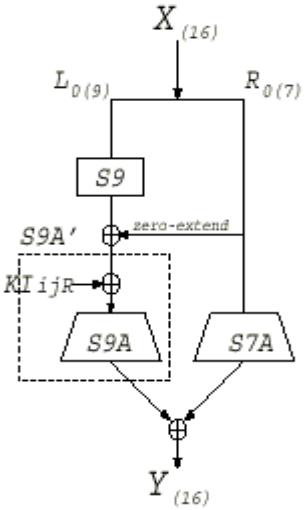
表 1. 置换表 S_7

451,203,339,415,483,233,251, 53,385,185,279,491,307, 9, 45,211,
199,330, 55,126,235,356,403,472,163,286, 85, 44, 29,418,355,280,
331,338,466, 15, 43, 48,314,229,273,312,398, 99,227,200,500, 27,
  1,157,248,416,365,499, 28,326,125,209,130,490,387,301,244,414,
467,221,482,296,480,236, 89,145, 17,303, 38,220,176,396,271,503,
231,364,182,249,216,337,257,332,259,184,340,299,430, 23,113, 12,
 71, 88,127,420,308,297,132,349,413,434,419, 72,124, 81,458, 35,
317,423,357, 59, 66,218,402,206,193,107,159,497,300,388,250,406,
481,361,381, 49,384,266,148,474,390,318,284, 96,373,463,103,281,
101,104,153,336, 8, 7,380,183, 36, 25,222,295,219,228,425, 82,
265,144,412,449, 40,435,309,362,374,223,485,392,197,366,478,433,
195,479, 54,238,494,240,147, 73,154,438,105,129,293, 11, 94,180,
329,455,372, 62,315,439,142,454,174, 16,149,495, 78,242,509,133,
253,246,160,367,131,138,342,155,316,263,359,152,464,489, 3,510,
189,290,137,210,399, 18, 51,106,322,237,368,283,226,335,344,305,
327, 93,275,461,121,353,421,377,158,436,204, 34,306, 26,232, 4,
391,493,407, 57,447,471, 39,395,198,156,208,334,108, 52,498,110,
202, 37,186,401,254, 19,262, 47,429,370,475,192,267,470,245,492,
269,118,276,427,117,268,484,345, 84,287, 75,196,446,247, 41,164,
 14,496,119, 77,378,134,139,179,369,191,270,260,151,347,352,360,
215,187,102,462,252,146,453,111, 22, 74,161,313,175,241,400, 10,
426,323,379, 86,397,358,212,507,333,404,410,135,504,291,167,440,
321, 60,505,320, 42,341,282,417,408,213,294,431, 97,302,343,476,
114,394,170,150,277,239, 69,123,141,325, 83, 95,376,178, 46, 32,
469, 63,457,487,428, 68, 56, 20,177,363,171,181, 90,386,456,468,
 24,375,100,207,109,256,409,304,346, 5,288,443,445,224, 79,214,
319,452,298, 21, 6,255,411,166, 67,136, 80,351,488,289,115,382,
188,194,201,371,393,501,116,460,486,424,405, 31, 65, 13,442, 50,
 61,465,128,168, 87,441,354,328,217,261, 98,122, 33,511,274,264,
448,169,285,432,422,205,243, 92,258, 91,473,324,502,173,165, 58,
459,310,383, 70,225, 30,477,230,311,506,389,140,143, 64,437,190,
120, 0,172,272,350,292, 2,444,162,234,112,508,278,348, 76,450

表 2. 置换表 S_9

実装方法

参照プログラム（提出書類５）は、ここに記載した仕様をそのままの形で実現しています。
この他にも、ソフトウエアのスピードとメモリサイズのバランスにあわせて、MISTY1 は
さまざまは実装法が可能です。以下にソフトウエアによる高速化手法の一例を示します。



MISTY1 の FI 関数は左に示すように等価に変形することが
できます。ここで、S9A は 9 ビット入力 16 ビット出力の
テーブル、S9B は 7 ビット入力 16 ビット出力のテーブルです。
この時 Kij1 は他の鍵に吸収することができることに注意します。
この等価変形を用いると、テーブルサイズを増加させる代償に
演算量を減らすことができ、高速化できます。

さらに、KIijR は実際には 8 通りのバラエティしかないことに
注目すれば、点線内部を１つのテーブル S9A'と考えることにより
（したがってこのテーブルは８種類必要となる）、鍵スケジュール
の演算量を増加させる代償に演算量をさらに減らすことができ、
高速化できます。

バージョン情報

MISTY1 は以下に示す標準化活動に提案されています。これらに提案されたアルゴリズムは
本提案書に記述された MISTY1 と完全な互換性があります。

ISO / SC27　NESSIE　IETF-TLS

またMISTY1をハードウエア用にカスタマイズしたブロック暗号アルゴリズムKASUMIが
第三世代携帯電話（Ｗ－ＣＤＭＡ）の世界標準として採用されています。これはMISTY1を
ベースとして開発されましたが、MISTY1とは互換性がありません。

オブジェクト識別子

MISTY1 のオブジェクト識別子は RFC2994 "A Description of the MISTY1 Encryption
Algorithm" に記載されています。以下にその抜粋を示します。

The Object Identifier for MISTY1 in Cipher Block Chaining (CBC) mode is as follows:

MISTY1-CBC OBJECT IDENTIFIER ::=
  {iso(1) member-body(2) jisc(392)
  mitsubishi-electric-corporation(200011) isl(61) security(1)
  algorithm(1) symmetric-encryption-algorithm(1) misty1-cbc(1)}

MISTY1-CBC needs Initialization Vector (IV) as like as other algorithms, such as DES-CBC,
DES-EDE3-CBC and so on. To determine the value of IV, MISTY1-CBC takes parameter as:

MISTY1-CBC Parameter ::= IV

where IV ::= OCTET STRING -- 8 octets.

When this Object Identifier is used, plaintext is padded before encrypt it. At least 1 padding octet is appended at the end of the plaintext to make the length of the plaintext to the multiple of 8 octets. The value of these octets is as same as the number of appended octets. (e.g., If 5 octets are needed to pad, the value is 0x05.)

利用実績・推奨用途など

MISTY1 はその成立以来幅広い用途に使われています。以下にその一部を示します。
以下社名のないものは三菱電機製で、その情報は三菱電機の情報セキュリティ技術HP
http://www.security.melco.co.jp/ から得ることができます。

【ソフトウェア製品】
暗号ライブラリ＜PowerMISTY＞，認証ライブラリ＜CertMISTY＞，認証サーバシステム＜CERTMANAGER＞，ファイル暗号ソフトウエア＜CRYPTOFILE＞，セキュアWeb アクセス＜TRUSTWEB＞，メッセージ暗号ソフトウエア＜CRYPTOSIGN＞，ディジタルコンテンツ保護流通システム＜DIGICAPSULE＞，電子メイル・セキュリティ強化ツール＜魔法瓶II＞（ＮＴＴエレクトロニクス），ファイル暗号化ツールSecretStaff（三菱電機コントロールソフトウエア）
【ハードウェア製品】
LAN 暗号化装置＜MELWALL＞, 鍵管理装置＜MISTYKEYPER＞（三菱電機エンジニアリング）、暗号ＬＳＩCDI2050（米国：Cognitive Design, Inc），LSI開発用暗号アルゴリズムＩＰ