参考資料 76－2－6

一 般 社 団 法 人 電 波 産 業 会
デジタル放送システム開発部会
権利保護作業班／アクセス制御方式作業班

地上デジタル放送方式高度化の限定受信方式に関する中間報告（案）

目次

第 1 章　概要 2
第 2 章　背景 3
2.1　情報通信審議会放送システム委員会で示された要求条件 3
2.2　スクランブル方式の動向 3
2.3　量子計算機による暗号技術の危殆化 3
第 3 章　基本方針 5
第 4 章　地上放送高度化方式における限定受信方式 6
4.1　スクランブルサブシステム 6
4.1.1　スクランブル方式の暗号アルゴリズム 6
4.1.2　スクランブル手順 7
4.1.3　スクランブルの範囲 7
4.1.4　スクランブル方式に係る伝送制御信号 7
4.2　スクランブルサブシステムにおける暗号アルゴリズムの詳細 10
4.2.1　AES 暗号（鍵長 128 ビットの場合） 10
4.2.2　Camellia 暗号（鍵長 128 ビットの場合） 13
第 5 章　高度化放送導入方式（LDM 方式）における限定受信方式 17

第１章　概要

地上デジタルテレビジョン放送方式高度化の限定受信方式について、情報通信審議会放送システム委員会（以下、情通審と記す。）による要求条件およびスクランブル方式の動向調査結果を踏まえ、地上デジタルテレビジョン放送方式高度化に対応する限定受信方式の技術的条件を検討する際の基本方針を策定するとともに、スクランブルサブシステムに関する技術検討を行った。

用語・略語

CBC	Cipher Block Chaining
CTR	Counter
ISO BMFF	ISO Base Media File Format
CENC	MPEG Common Encryption
CMAF	Common Media Application Format

第 2 章　背景

2.1　情報通信審議会放送システム委員会で示された要求条件

（スクランブルサブシステム）

- 高度な秘匿性を有すること。
- 不正受信に対して十分な安全性を有し、脆弱性が発見された場合等に対応できる機能を有すること。

2.2　スクランブル方式の動向

米国 ATSC3.0、韓国 ATSC3.0（4K 地上放送）、DVB、及び日本におけるスクランブル方式の比較を表 1 に示す。世界的に ISO BMFF 対応が進んでいるほか、通信で標準的なスクランブル方式である CENC が一部の放送システムで採用されている。

表 1　スクランブル方式の比較

諸外国の方式	ATSC3.0（米国）	ATSC3.0（韓国）	DVB	Google（Widevine CAS）
スクランブル対象	ISO BMFF	ISO BMFF	MPEG2-TS／PES	MPEG2-TS、ISO BMFF
スクランブル方式（暗号方式）	CENC (AES)	CENC (AES)	DVB-CSA (AES等)	各放送方式にカスタマイズ対応

日本方式	地上（B-CAS方式）	地上（TRMP方式）	新4K8K衛星放送
スクランブル対象	MPEG2-TS		MMTPパケット
スクランブル方式（暗号方式）	告示 (MULTI-2)		告示 (AES／Camellia)

通信のストリーミングでは、暗号利用モードの対応が DRM 毎に分かれており、CTR モードだけでなく CBC モードの採用も進んでいる（表 2）。

表 2　DRM 別の暗号利用モードの対応状況

DRM	AES-CTRモード	AES-CBCモード
Widevine (Google)	○	○
FairPlay (Apple)	×	○
PlayReady (Microsoft) V4.0以降	○	○
PlayReady (Microsoft) V1.0～3.3	○	×
WisePlay (Huawei)	○	○

2.3　量子計算機による暗号技術の危殆化

近年、量子計算機の開発が盛んに行われているが、将来大規模な量子計算機が出現すると、既存の暗号方式が危殆化する（安全でなくなる）ことが知られている。新 4K8K 衛星放送では、暗号方式として鍵長 128 ビットの AES または鍵長 128 ビットの Camellia のいずれかを選択または切り替えで

きるようになっており、現時点において安全性に問題はない。しかし、AES や Camellia などの共通鍵暗号方式は、量子計算機を用いると鍵の全数探索を高速に実行可能なアルゴリズムが知られているため、長期的に保護したいデータには鍵長 128 ビットの暗号方式ではなく、192 ビットや 256 ビットの暗号技術を使用するのが賢明であると考えられている※1。そのため、地上デジタルテレビジョン放送方式高度化に対応するスクランブル方式についても、新 4K8K 衛星放送と同様に鍵長 128 ビットの暗号方式を用いるか、それとも 192 ビットや 256 ビットの暗号技術を用いるか検討する必要がある。

※1：https://www.cryptrec.go.jp/exreport/cryptrec-ex-2901-2019.pdf　CRYPTREC 外部評価報告書（2019 年度）「量子コンピュータが共通鍵暗号の安全性に及ぼす影響の調査及び評価」エグゼクティブサマリー

第 3 章　基本方針

第 2 章の背景を踏まえ、地上デジタルテレビジョン放送方式高度化に対応する限定受信方式の技術的条件を検討する際の基本方針を以下のように定める。

① 地上デジタルテレビジョン放送方式高度化におけるサービス要件が現時点で決まっていないため、関連情報サブシステムについては議論せず、スクランブルサブシステムのみを検討する。
② 新 4K8K 衛星放送で採用されているスクランブル方式をベースに検討するが、諸外国の標準化動向を踏まえ、通信で用いられているスクランブル方式の採用可否についても検討する。
③ 暗号方式については、現時点での安全性だけでなく将来を見据えた安全性を考慮する。
④ 受信機コストや現行放送システムとの互換性確保などの実現可能性についても考慮する。

第 4 章　地上放送高度化方式における限定受信方式

4.1　スクランブルサブシステム

第 3 章の基本方針に従い、地上放送高度化方式における限定受信方式のうちスクランブルサブシステムに関する技術検討を行った。

4.1.1　スクランブル方式の暗号アルゴリズム

放送システム委員会が示した地上デジタルテレビジョン放送方式高度化におけるスクランブルサブシステムの要求条件（2.1 節参照）は、新 4K8K 衛星放送の要求条件から特に変更は無く、暗号方式などの情報セキュリティに関しては新 4K8K 衛星放送と同等またはそれ以上のレベルであれば問題ないと考えられる。

新 4K8K 衛星放送のスクランブル方式が使用する暗号アルゴリズムは、CRYPTREC（Cryptography Research and Evaluation Committees：電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト）で公表されている電子政府推奨暗号リスト※2に掲載されている AES 128 ビットブロック暗号または Camellia 128 ビットブロック暗号であり、これらのいずれかを選択または切り替えできるようになっている（実際の放送では、ARIB 運用規定により AES の運用に制限されている）。一方、通信で標準的なスクランブル方式である CENC では、暗号アルゴリズムとして AES が用いられている。従って、地上デジタルテレビジョン放送方式高度化におけるスクランブル方式で使用する暗号アルゴリズムは、新 4K8K 衛星放送と同様、法令や民間規格では AES と Camellia の両方を規定し、通信の動向を確認しながら運用を絞ることが望ましい。

※2：https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r7.pdf　電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）

なお、新 4K8K 衛星放送のスクランブル方式や CENC で用いられている暗号アルゴリズムでは鍵長 128 ビットが採用されているが、AES、Camellia ともに鍵長は 128 ビット、192 ビット、256 ビットの 3 種類から選択できるようになっている。現時点では鍵長 128 ビットでも安全性に問題はないが、2.3 節で述べた量子計算機による将来的な暗号アルゴリズムの危殆化を鑑み、鍵長 192 ビットや 256 ビットの暗号アルゴリズムを用いるかどうかについても検討する必要がある。鍵長を選択する際には、CRYPTREC で公表されている暗号強度要件に関する設定基準※3 等を踏まえ、適切なセキュリティ強度を実現するための鍵長を選択することが望ましい（基本方針③）。

※3：https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf　暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準

スクランブル方式の暗号アルゴリズムの選定にあたっては、以下の各項に留意することが望ましい。

- スクランブル方式は、暗号アルゴリズム自身の安全性だけではなく、受信機における実装面、コスト面、および実用化スケジュール、ならびに、長期にわたってセキュリティリスクを抑える送

出運用などに考慮して、民間規格や運用検討の場において、放送事業者や受信機製造メーカなどの関係者で最終的に選定する必要がある（基本方針④）。

・ 長期視点で見ると、より効率的な暗号解析手法が見つかる可能性も否定できない。CRYPTREC の電子政府推奨暗号リストの改定など、暗号アルゴリズムの最新動向に今後留意する必要があり、民間規格や運用検討の場において、必要に応じて議論・検討する必要がある（基本方針③）。

4.1.2 スクランブル手順

新 4K8K 衛星放送では CTR モードのみ対応しているが、通信のストリーミングにおいて今後も CBC モードを使用する流れになる場合、共用受信機（BS4K8K、地上 2K、地上 4K、通信の各コンテンツを視聴できる受信機）は CTR モードと CBC モードの両方をサポートする必要がある。従って、法令や民間規格では CTR モードと CBC モードの両方を規定し、通信の動向を確認しながら運用を判断することが望ましい（基本方針②）。

4.1.3 スクランブルの範囲

多重化方式におけるメディアデータの伝送方式に応じてスクランブルの範囲が異なる。

新 4K8K 衛星放送と同じ MMT・TLV 方式の場合、MMTP パケットの MMTP ペイロードのデータ部がスクランブルの範囲となる。

多重化方式の提案方式の一つである CMAF･MMT･TLV 方式の場合、スクランブルを施す階層は、MMTP パケットの MMTP ペイロードのデータ部および CMAF となる。スクランブルの範囲および階層は表 3 に示す 4 つの組み合わせが考えられるが、それぞれ利点・欠点があるため慎重な検討が必要である。

表 3　スクランブルの範囲および階層

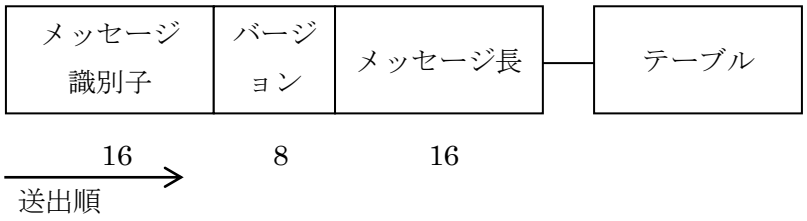
No	MMTPペイロード	CMAF	備考
1	暗号化（スクランブル）	非暗号	新4K8K衛星放送と同じ
2	暗号化（スクランブル）	CENCで暗号化	2重の暗号化
3	非暗号	非暗号	いわゆるノンスクランブル運用
4	非暗号	CENCで暗号化	通信の暗号化と同じ

なお、CMAF を CENC で暗号化する場合は受信機に DRM の復号モジュールが必要であり、通信経由で復号鍵をライセンスサーバに問い合わせる手法が一般的である。しかし、通信機能の有無にかかわらず通信に接続していないテレビの存在も想定する必要があり、通信を利用しなくても CMAF を復号できるスクランブル方式についても検討する必要がある（基本方針②）。

4.1.4 スクランブル方式に係る伝送制御信号

地上デジタルテレビジョン放送方式高度化のスクランブル方式で複数の暗号アルゴリズムを採用する場合、新 4K8K 衛星放送と同様に、スクランブルサブシステムの識別のために、図 1(a)に示す伝送制御信号（CA メッセージ）に配置される CA テーブル（図 1(b)）に配置可能な記述子として、スクランブル方式記述子（図 2）を規定する必要がある（基本方針②）。

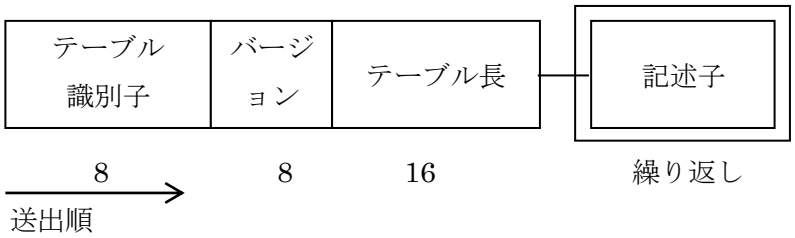
なお、新 4K8K 衛星放送では、放送と通信を組み合わせたコンテンツ配信を想定し、パケットの改ざんを防止できるメッセージ認証方式（改ざん検出のために、パケット単位にメッセージ認証コードを付与する仕組み）が導入されており、そのメッセージ認証方式を識別するメッセージ認証方式記述子（図 3）が規定されている（実際の放送では、ARIB 運用規定によりメッセージ認証方式は運用されていない）。地上デジタルテレビジョン放送方式高度化のスクランブル方式においても、メッセージ認証方式の導入可否の検討が必要である（基本方針②）。



注 1）メッセージ識別子の値は、CA メッセージを示す 0xXXXX とする。

注 2）テーブル領域には、CA テーブルが配置される。

図 1(a)：CA メッセージの構成



注 1）テーブル識別子の値は、CA テーブルを示す 0xXX とする。

図 1(b)：CA テーブルの構成

記述子タグ	記述子長	対象レイヤー識別子	“111111”	スクランブル方式識別子	データ
16	8	2	6	8	8×N

注 1）記述子タグの値は、スクランブル方式記述子を示す 0xXXXX とする。

注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。

注 3）対象レイヤー識別子は、スクランブル時の暗号化対象（IP パケット、MMT パケット）を示す。

注 4）スクランブル方式識別子は、スクランブル時の暗号アルゴリズムの種別を示す。

注 5）本記述子は、CA メッセージの CA テーブルの記述子領域又は MP テーブルの MPT ディスクリプタ領域若しくは MP テーブルのアセットディスクリプタ領域で伝送するものとする。

図 2：スクランブル方式記述子の構成

記述子タグ	記述子長	対象レイヤー識別子	“111111”	メッセージ認証方式識別子	データ
16	8	2	6	8	8×N

注 1）記述子タグの値は、メッセージ認証方式記述子を示す 0xXXXX とする。
注 2）記述子長は、これより後に続くデータバイト数を書き込む領域とする。
注 3）対象レイヤー識別子は、MMT パケットまたは IP パケットの改ざん検出を行うメッセージ認証の対象（IP パケット、MMT パケット）を示す。
注 4）メッセージ認証方式識別子は、MMT パケットまたは IP パケットの改ざん検出を行うメッセージ認証方式の種別を示す。
注 5）本記述子は、CA メッセージの CA テーブルの記述子領域又は MP テーブルの MPT ディスクリプタ領域若しくは MP テーブルのアセットディスクリプタ領域で伝送するものとする。

図 3：メッセージ認証方式記述子の構成

表 4：スクランブル方式識別子の値の割当て

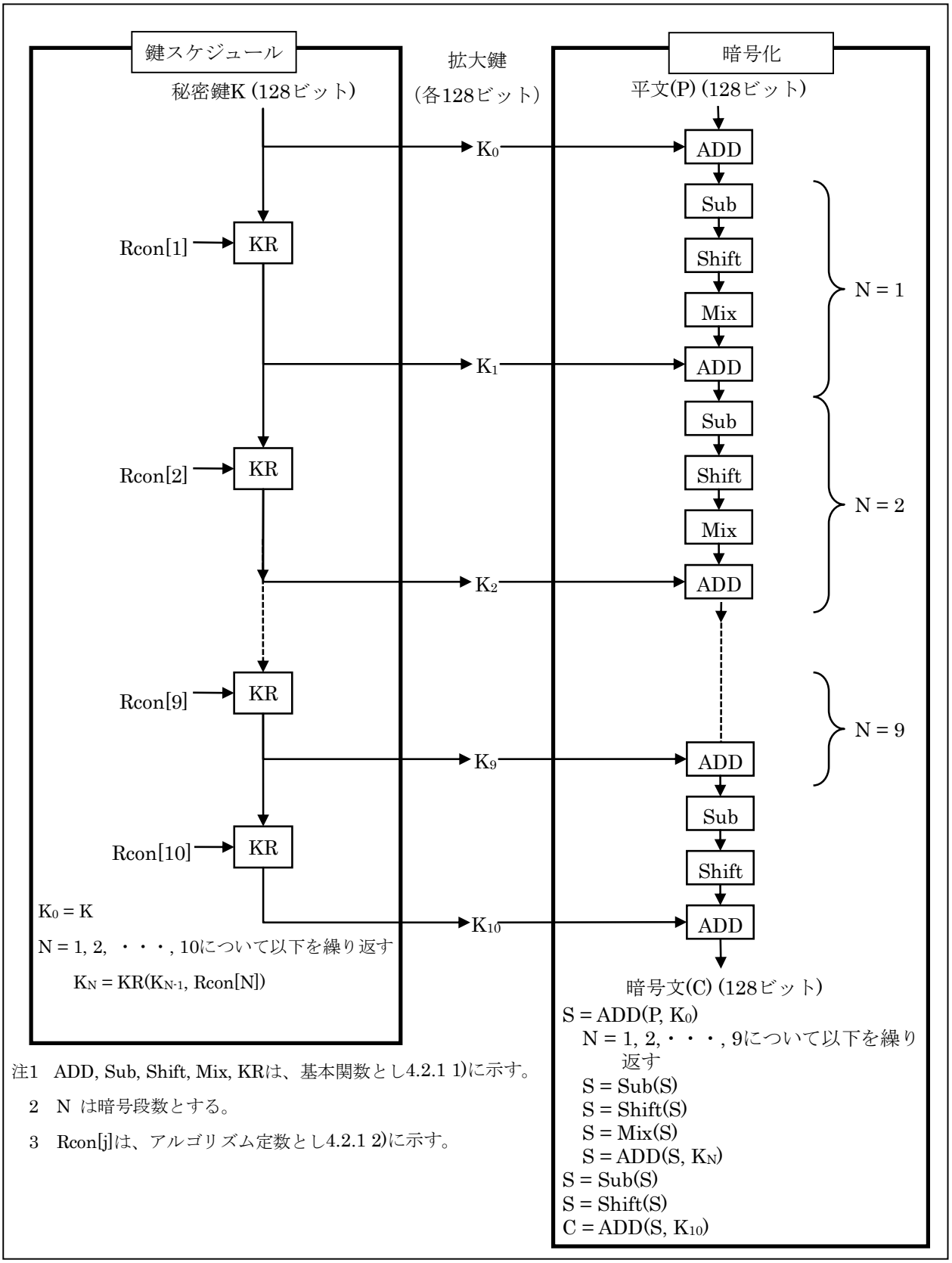
値（2 進数）	割当て
00000000	未定義
00000001	AES、鍵長 128 ビット
00000010	Camellia、鍵長 128 ビット
00000011 - 11111111	未定義

表 5：対象レイヤー識別子の値の割当て

値（2 進数）	割当て
00	未定義
01	MMT パケットを対象
10	IP パケットを対象
11	未定義

4.2　スクランブルサブシステムにおける暗号アルゴリズムの詳細

4.2.1　AES 暗号（鍵長 128 ビットの場合）



注1　ADD, Sub, Shift, Mix, KRは、基本関数とし4.2.1 1)に示す。

2　N は暗号段数とする。

3　Rcon[j]は、アルゴリズム定数とし4.2.1 2)に示す。

図 4

1）基本関数

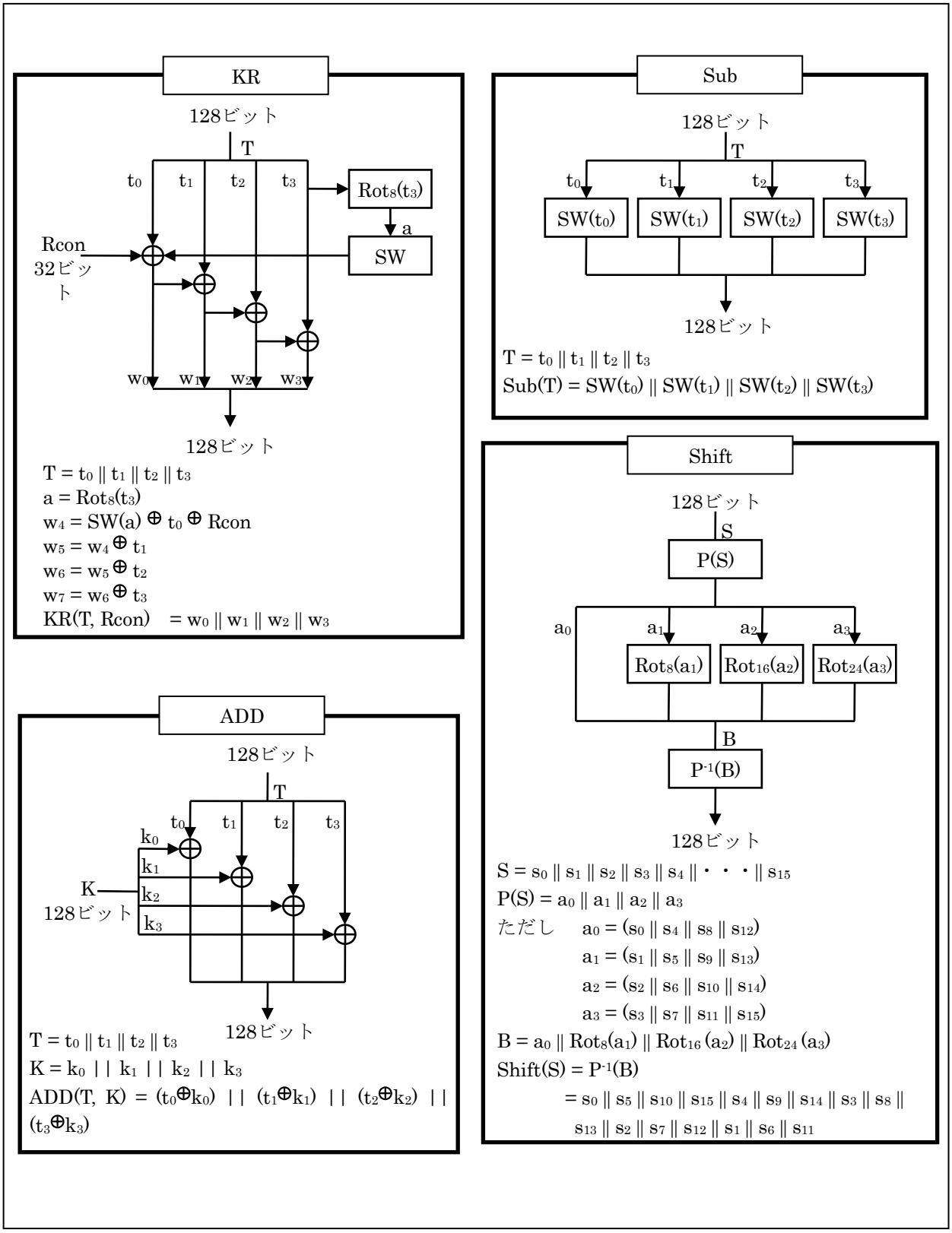
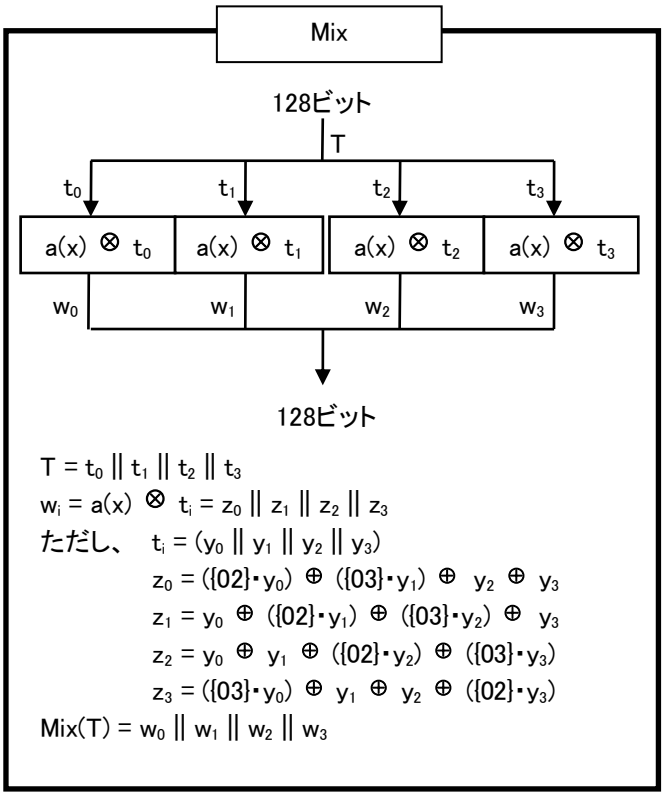

KR
128ビット
T
t0 t1 t2 t3
Rot8(t3)
a
SW
Rcon
32ビット
w0 w1 w2 w3
128ビット
T = t0 || t1 || t2 || t3
a = Rot8(t3)
w4 = SW(a) ⊕ t0 ⊕ Rcon
w5 = w4 ⊕ t1
w6 = w5 ⊕ t2
w7 = w6 ⊕ t3
KR(T, Rcon) = w0 || w1 || w2 || w3
Sub
128ビット
T
t0 t1 t2 t3
SW(t0) SW(t1) SW(t2) SW(t3)
128ビット
T = t0 || t1 || t2 || t3
Sub(T) = SW(t0) || SW(t1) || SW(t2) || SW(t3)
Shift
128ビット
S
P(S)
a0 a1 a2 a3
Rot8(a1) Rot16(a2) Rot24(a3)
B
P-1(B)
128ビット
S = s0 || s1 || s2 || s3 || s4 || ・・・ || s15
P(S) = a0 || a1 || a2 || a3
ただし a0 = (s0 || s4 || s8 || s12)
a1 = (s1 || s5 || s9 || s13)
a2 = (s2 || s6 || s10 || s14)
a3 = (s3 || s7 || s11 || s15)
B = a0 || Rot8(a1) || Rot16 (a2) || Rot24 (a3)
Shift(S) = P-1(B)
= s0 || s5 || s10 || s15 || s4 || s9 || s14 || s3 || s8 ||
s13 || s2 || s7 || s12 || s1 || s6 || s11
ADD
128ビット
T
t0 t1 t2 t3
k0 k1 k2 k3
K
128ビット
128ビット
T = t0 || t1 || t2 || t3
K = k0 || k1 || k2 || k3
ADD(T, K) = (t0⊕k0) || (t1⊕k1) || (t2⊕k2) || (t3⊕k3)

図 5

注1　Tは、基本関数への入力とする。
2　⊕は、ビット毎の排他的論理和とする。
3　‖ は、ブロックの結合とする。
4　SWは、補助関数とし3.3.1 2)に示す。
5　Rot_n は、左巡回nビットシフトとする。
6　・は、GF(2^8)上の乗算を表す。
既約多項式は、
$x^8 + x^4 + x^3 + x + 1$とする。



$T = t_0 \| t_1 \| t_2 \| t_3$
$w_i = a(x) \otimes t_i = z_0 \| z_1 \| z_2 \| z_3$
ただし、 $t_i = (y_0 \| y_1 \| y_2 \| y_3)$
$z_0 = (\{02\} \cdot y_0) \oplus (\{03\} \cdot y_1) \oplus y_2 \oplus y_3$
$z_1 = y_0 \oplus (\{02\} \cdot y_1) \oplus (\{03\} \cdot y_2) \oplus y_3$
$z_2 = y_0 \oplus y_1 \oplus (\{02\} \cdot y_2) \oplus (\{03\} \cdot y_3)$
$z_3 = (\{03\} \cdot y_0) \oplus y_1 \oplus y_2 \oplus (\{02\} \cdot y_3)$
$Mix(T) = w_0 \| w_1 \| w_2 \| w_3$

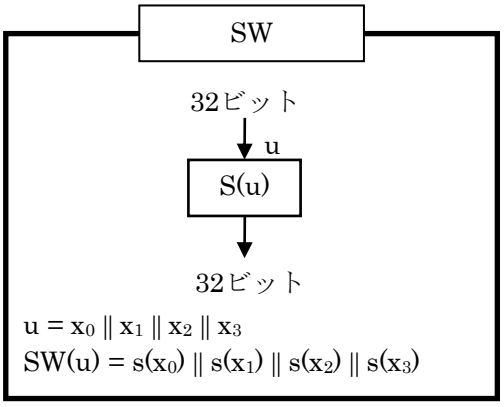
図 6

2）アルゴリズム定数と補助関数

アルゴリズム定数

Rcon[1] = 01000000
Rcon[2] = 02000000
Rcon[3] = 04000000
Rcon[4] = 08000000
Rcon[5] = 10000000
Rcon[6] = 20000000
Rcon[7] = 40000000
Rcon[8] = 80000000
Rcon[9] = 1b000000
Rcon[10] = 36000000
注　数値は16進表記とする。

補助関数

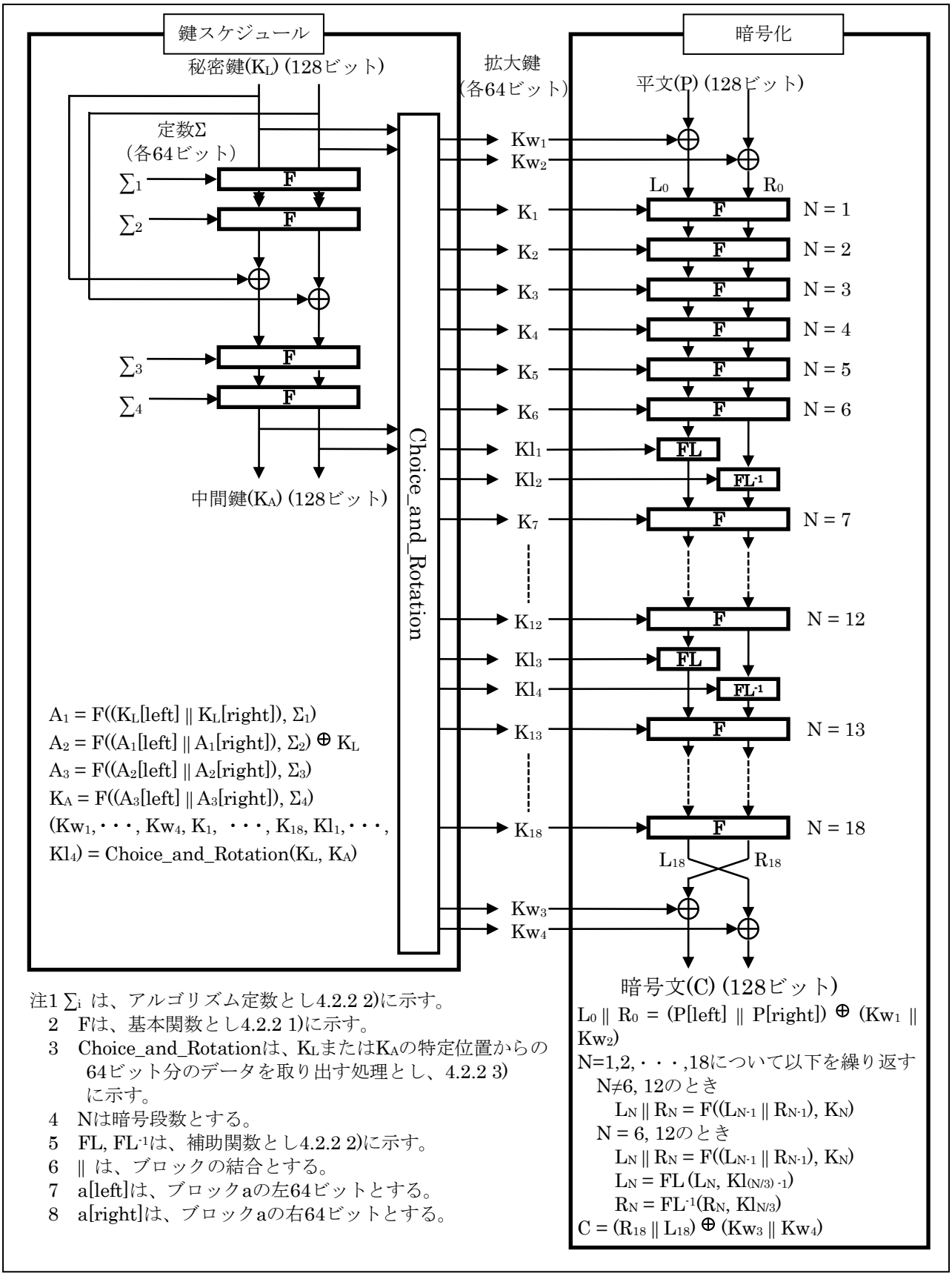


$u = x_0 \| x_1 \| x_2 \| x_3$
$SW(u) = s(x_0) \| s(x_1) \| s(x_2) \| s(x_3)$

注1　u は、補助関数への入力とする。
2　‖ は、ブロックの結合とする。
3　s は、8ビットの置換表とし、詳細は ISO/IEC 18033-3 に従うものとする。

図 7

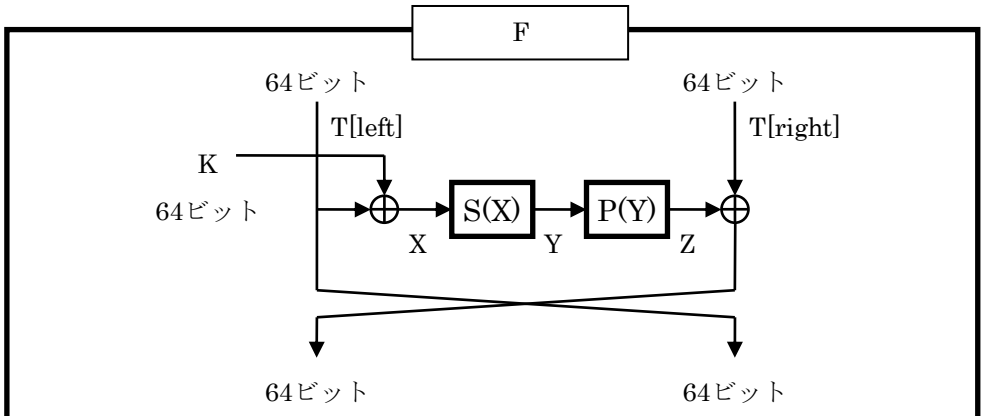
4.2.2　Camellia 暗号（鍵長 128 ビットの場合）



注1 $\sum_i$ は、アルゴリズム定数とし4.2.2 2)に示す。
2　Fは、基本関数とし4.2.2 1)に示す。
3　Choice_and_Rotationは、K_LまたはK_Aの特定位置からの64ビット分のデータを取り出す処理とし、4.2.2 3)に示す。
4　Nは暗号段数とする。
5　FL, FL^{-1}は、補助関数とし4.2.2 2)に示す。
6　|| は、ブロックの結合とする。
7　a[left]は、ブロックaの左64ビットとする。
8　a[right]は、ブロックaの右64ビットとする。

図 8

1）基本関数



$X = T[left] \oplus K = (x_8 \| x_7 \| x_6 \| x_5 \| x_4 \| x_3 \| x_2 \| x_1)$

$Y = S(X) = (s_1(x_8) \| s_4(x_7) \| s_3(x_6) \| s_2(x_5) \| s_4(x_4) \| s_3(x_3) \| s_2(x_2) \| s_1(x_1))$

$= (y_8 \| y_7 \| y_6 \| y_5 \| y_4 \| y_3 \| y_2 \| y_1)$

$Z = P(Y) = (z_8 \| z_7 \| z_6 \| z_5 \| z_4 \| z_3 \| z_2 \| z_1)$

ただし

$z_1 = y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8$

$z_2 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8$

$z_3 = y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8$

$z_4 = y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$

$z_5 = y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8$

$z_6 = y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8$

$z_7 = y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8$

$z_8 = y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7$

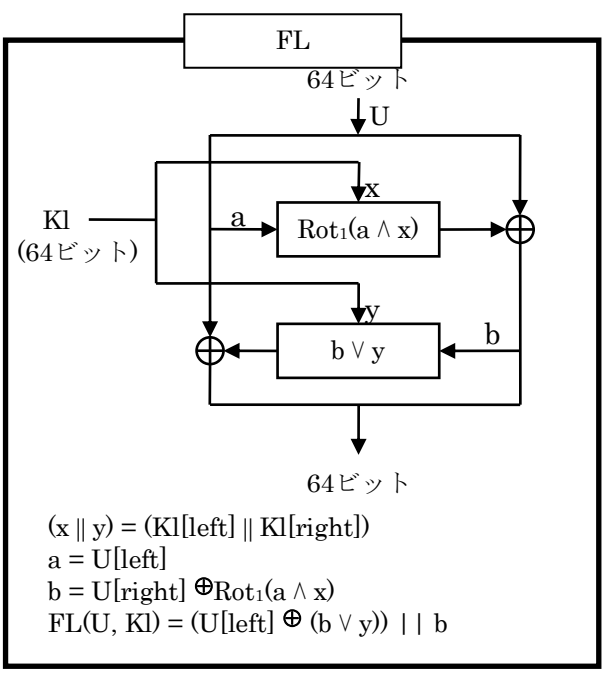
$F(T, K) = (T[right] \oplus Z) \| T[left]$

注1　Tは、基本関数への入力とする。
2　T[left]は、ブロックTの左64ビットとする。
3　T[right]は、ブロックTの右64ビットとする。
4　‖ は、ブロックの結合とする。
5　s_i は、8ビットの置換表とし、詳細はISO/IEC18033-3:2005(E) 5.2.3.4節に従うこととする。

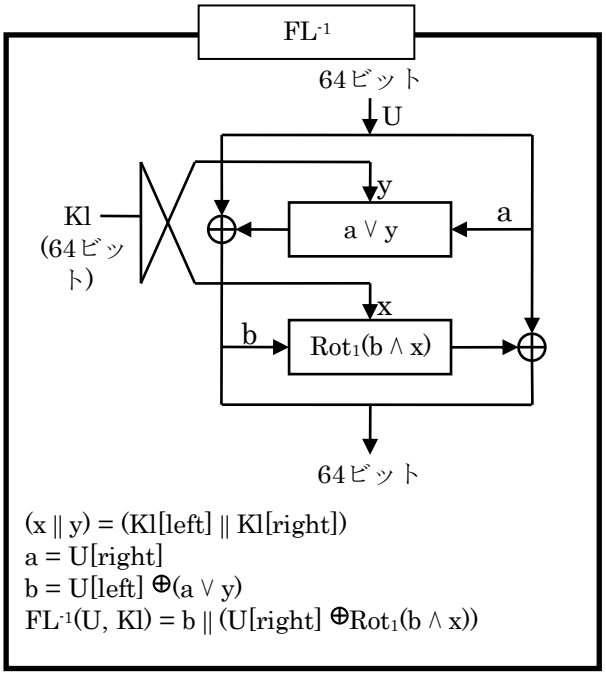
図 9

2）補助関数とアルゴリズム定数

補助関数



(x || y) = (Kl[left] || Kl[right])
a = U[left]
b = U[right] ⊕Rot1(a ∧ x)
FL(U, Kl) = (U[left] ⊕ (b ∨ y)) || b



(x || y) = (Kl[left] || Kl[right])
a = U[right]
b = U[left] ⊕(a ∨ y)
FL-1(U, Kl) = b || (U[right] ⊕Rot1(b ∧ x))

注1　Uは、補助関数への入力とする。
　2　 || は、ブロックの結合とする。
　3　Rot1 は、左巡回1ビットシフトとする。
　4　∧ は、ビット毎の論理積とする。
　5　∨ は、ビット毎の論理和とする。
　6　U[left]は、ブロックUの左32ビットとする。
　7　U[right]は、ブロックUの右32ビットとする。

アルゴリズム定数

Σ_1 = a09e667f3bcc908b

Σ_2 = b67ae8584caa73b2

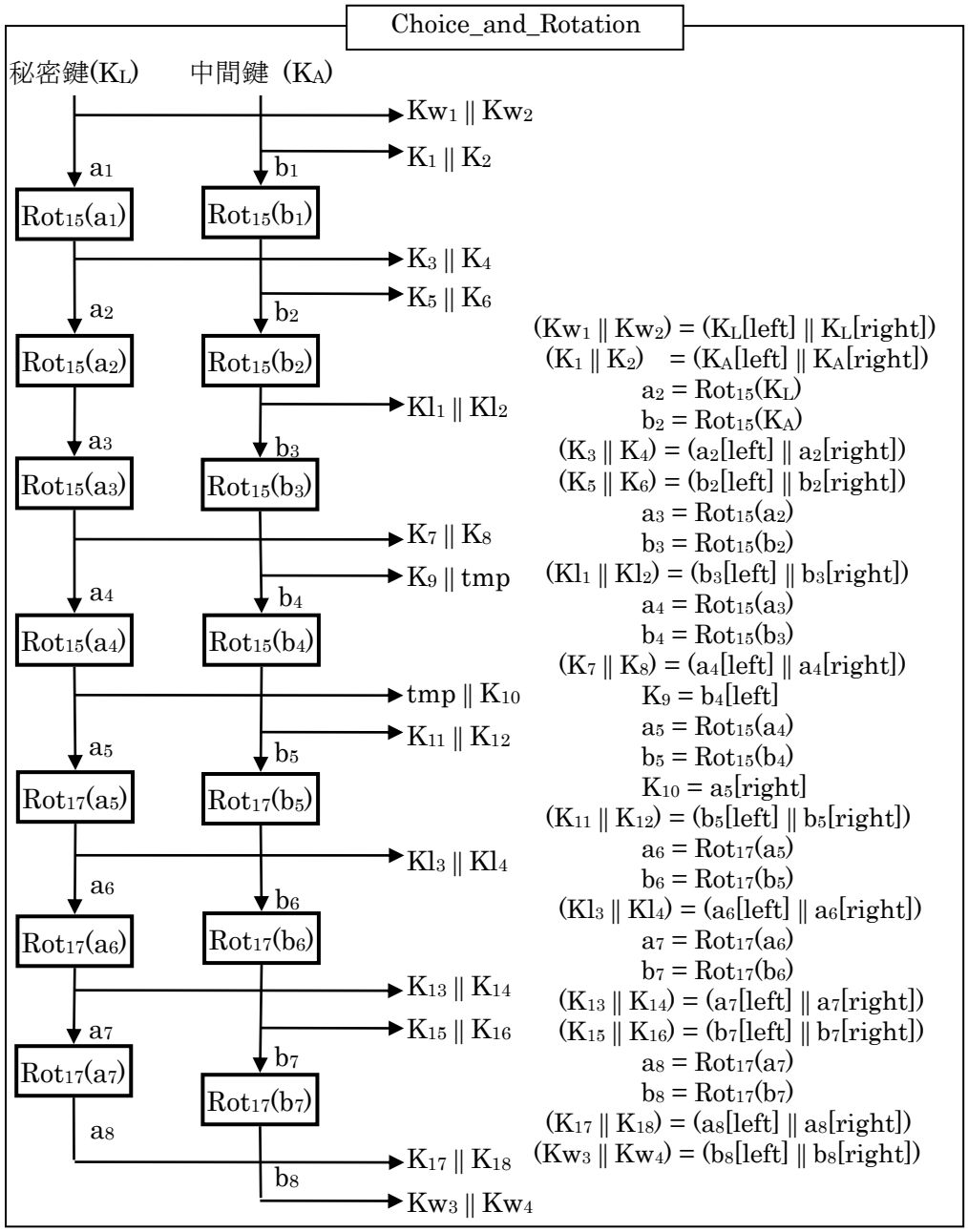
Σ_3 = c6ef372fe94f82be

Σ_4 = 54ff53a5f1d36f1c

注　数値は16進表記とする。

図 10

3）Choice_and_Rotation



注1　U[left]は、ブロックUの左64ビットとする。
　2　U[right]は、ブロックUの右64ビットとする。
　3　 || は、ブロックの結合とする。
　4　Rot_n は、左巡回nビットシフトとする。

図 11

第５章　高度化放送導入方式（LDM 方式）における限定受信方式

限定受信方式は伝送路符号化方式の違いによって影響を受けるものではないため、高度化放送導入方式（LDM 方式）における限定受信方式については、地上放送高度化方式における限定受信方式と同一のものとすることが適当と考える。