デ高作 19－4－6

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

高度地上デジタルテレビジョン放送方式
適用技術検討報告
限定受信方式

2023 年 2 月 27 日

3.4　限定受信方式

限定受信方式について、高度地上デジタルテレビジョン放送方式の要求条件を踏まえ、スクランブルサブシステムに関する技術検討を行った。現行の 4K8K 衛星放送と同じく、複数の暗号アルゴリズムから選択可能とする方式とし、多重化レベルで暗号アルゴリズムを指定する記述子などを導入することとした。具体的には、暗号アルゴリズムは、CRYPTREC で公表されている電子政府推奨暗号リストを参考に、AES 128 ビットブロック暗号及び Camellia 128 ビットブロック暗号から選択可能とするとともに、鍵長を 128 ビット、192 ビット、256 ビットから選択可能とした。また、スクランブル方式の暗号アルゴリズムを指定する記述子としてスクランブル方式記述子を導入するとともに、通信利用を考慮してメッセージ認証方式記述子を検討した。さらに、現行放送（4K8K 衛星放送）の多重化方式に加え、放送コンテンツのメディアアプリケーションフォーマットを ISO/IEC 23000-19(Common media application format(CMAF))の規定に基づくものとする多重化方式を想定し、現行の 4K8K 衛星放送のスクランブル方式、及び CMAF のスクランブル方式である MPEG Common Encryption (CENC)いずれも対応可能となるように、スクランブル手順及びスクランブルの範囲を検討した。

3.4.1　スクランブルサブシステム

3.4.1.1　スクランブル方式の暗号アルゴリズム

スクランブル方式の暗号アルゴリズムに関しては、AES 128 ビットブロック暗号及び Camellia 128 ビットブロック暗号を選択可能とする。

鍵長に関しては、128 ビット、192 ビット、256 ビットのいずれかを選択可能とする。

（理由）

暗号アルゴリズム： 現行の 4K8K 衛星放送との整合性を確保するため。

鍵長： 計算機の性能向上および大規模な量子計算機による将来的な安全性の低下を考慮したため。

暗号アルゴリズムに関しては、現行の 4K8K 衛星放送との整合性を確保するため、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）の電子政府推奨暗号リスト※1 に掲載されている AES 128 ビットブロック暗号及び Camellia 128 ビットブロック暗号を採用した。この電子政府推奨暗号リストは、最新・最先端の暗号解析結果を基にして、専門家により安全性評価、実装評価及び利用実績の評価が行われ、推奨暗号としてまとめられたもので、暗号アルゴリズムの選定にあたっては大きな指標となる。また、現行の 4K8K 衛星放送と同様、暗号アルゴリズムに脆弱性が発見された場合を考慮し、AES、Camellia いずれかを選択または切り替えできるようにした。

※1：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）

鍵長に関しては、計算機の性能向上および大規模な量子計算機による将来的な安全性の低下を考慮し、現行の 4K8K 衛星放送で採用されている 128 ビットに加え、192 ビット、256 ビットを選択できるようにした。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※2 等を踏まえ、適切なセキュリティ強度を実現する鍵長を選択することが望ましい。

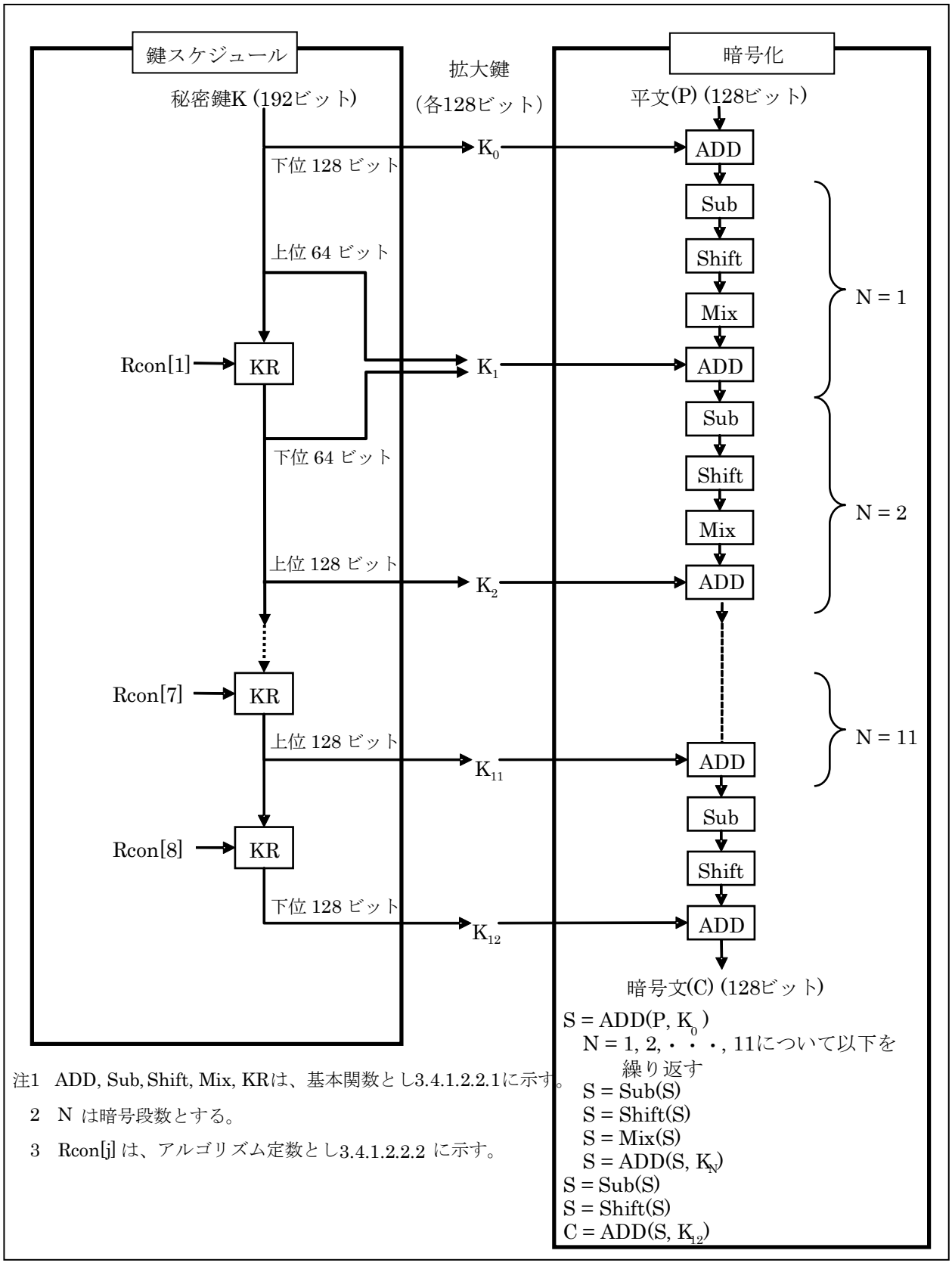
※2:https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022.pdf　暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準

3.4.1.2　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

3.4.1.2.1　AES 暗号（鍵長 128 ビットの場合）

鍵長 128 ビットの場合の AES 暗号は、平成 26 年総務省告示第 235 号別表第二号別記第 1～別記第 4 に基づくものとする。

3.4.1.2.2　AES 暗号（鍵長 192 ビットの場合）



注1　ADD, Sub, Shift, Mix, KRは、基本関数とし3.4.1.2.2.1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3.4.1.2.2.2 に示す。

図 3.4.1.2.2-1　AES 暗号のアルゴリズム（鍵長 192 ビットの場合）

3.4.1.2.2.1　基本関数

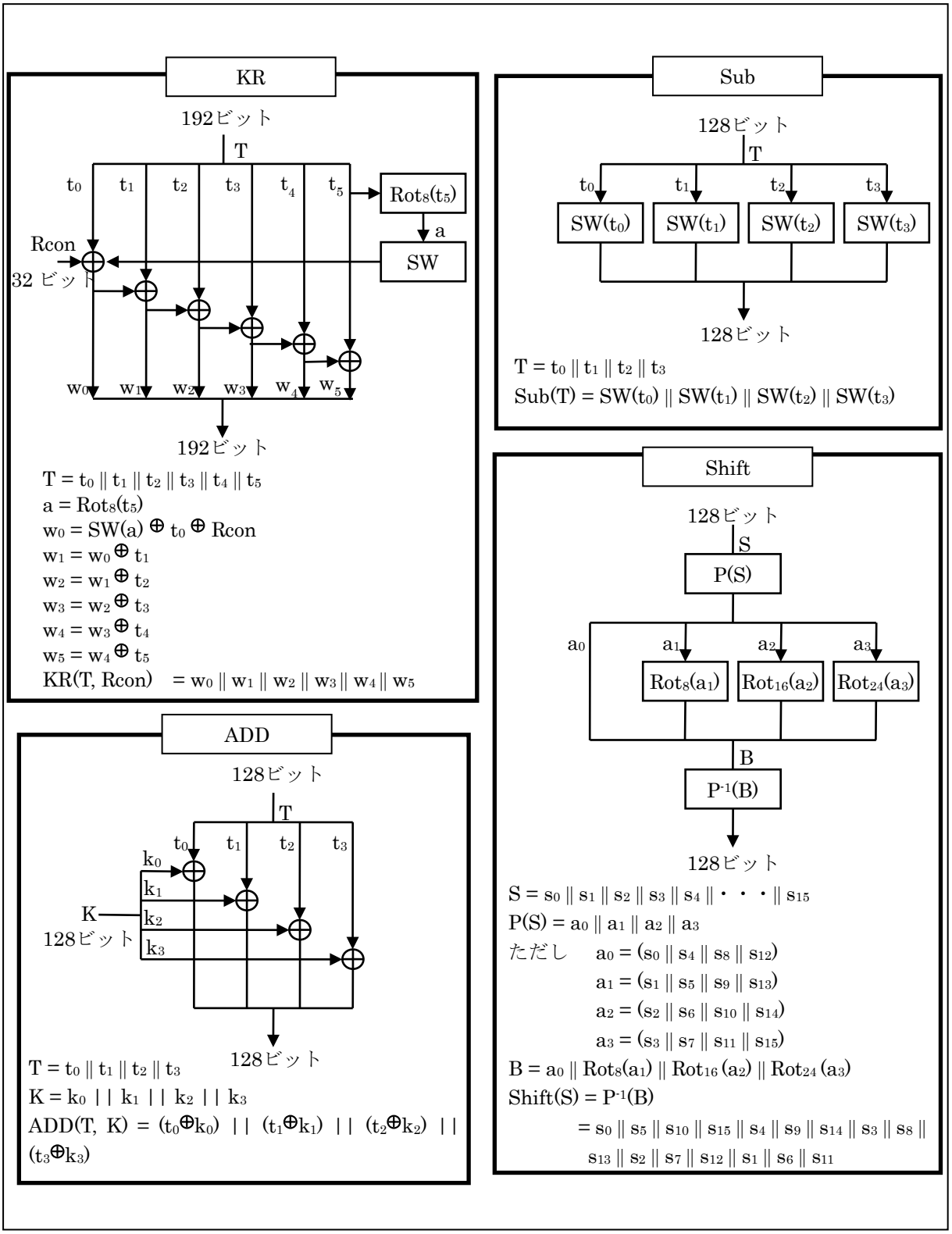


図 3.4.1.2.2.1-1　AES 暗号の基本関数（鍵長 192 ビットの場合）

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3.4.1.2.2.2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。

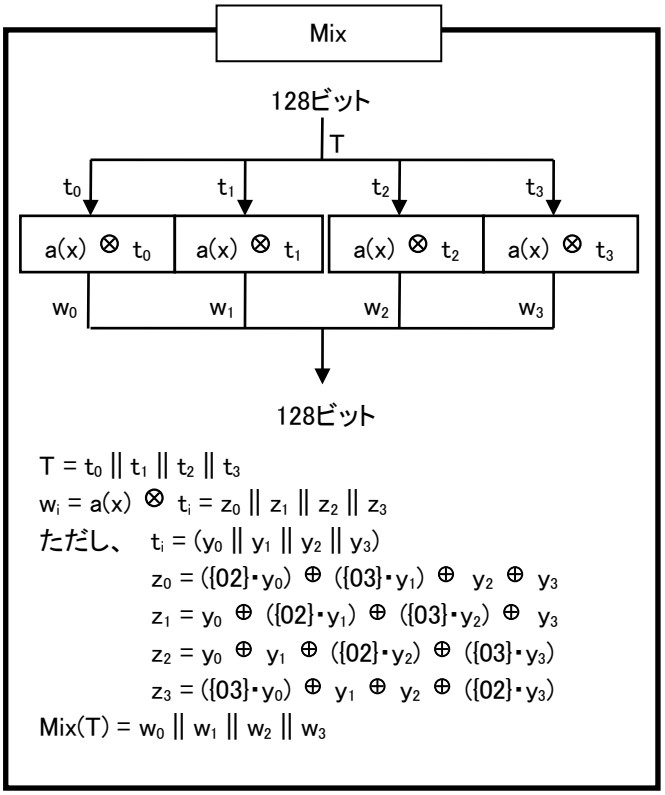


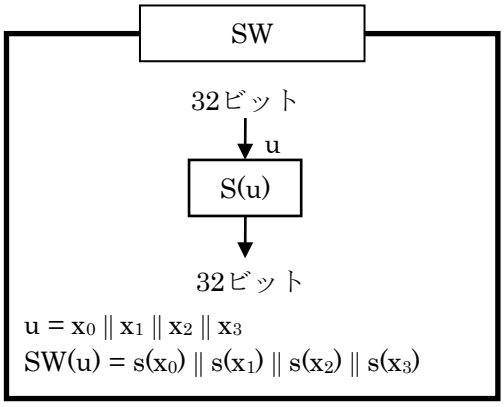
図 3.4.1.2.2.1-2　AES 暗号の基本関数（鍵長 192 ビットの場合）

3.4.1.2.2.2　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
注　数値は16進表記とする。

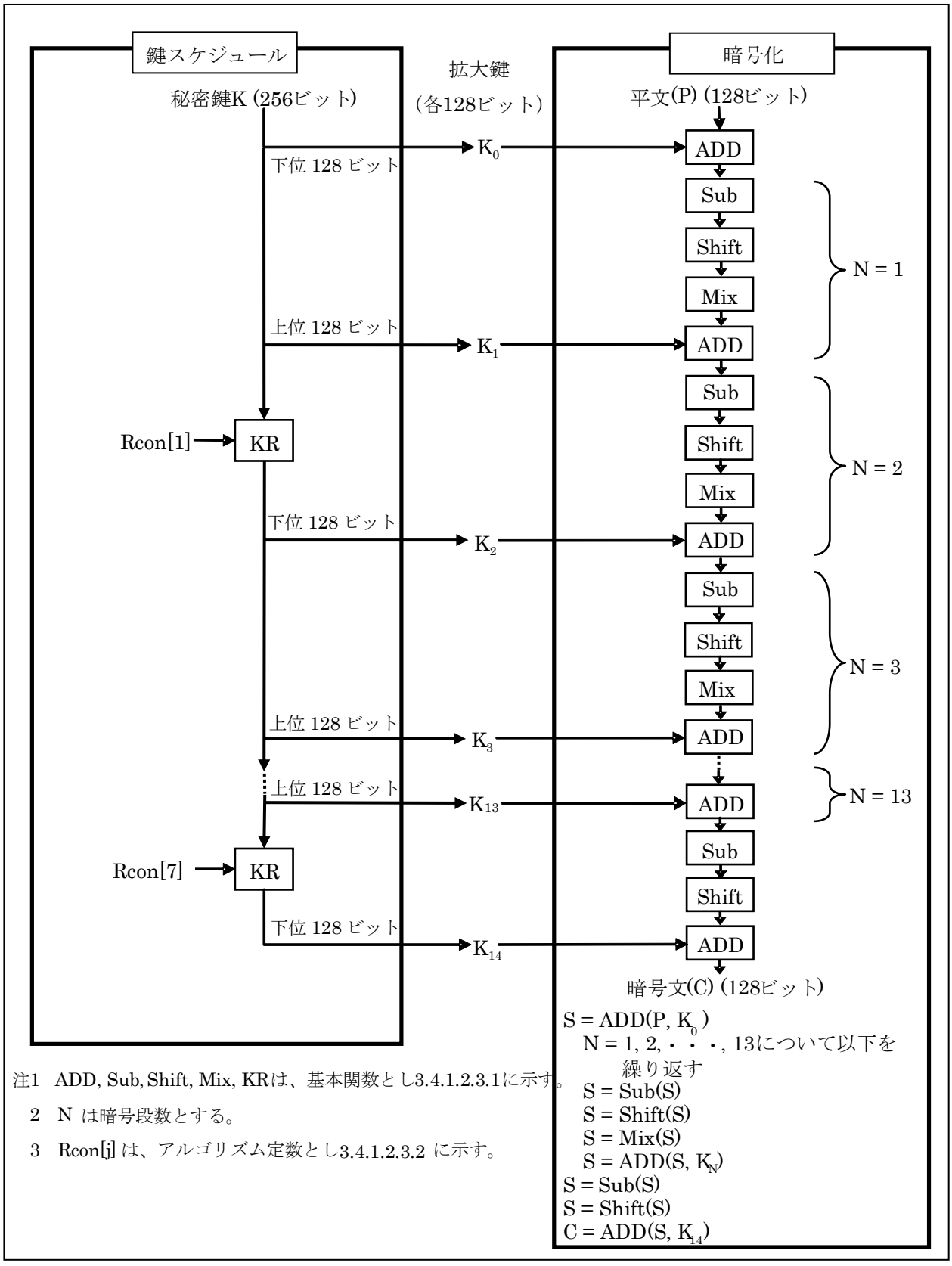
補助関数



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 3.4.1.2.2.2-1　AES 暗号のアルゴリズム定数と補助関数（鍵長 192 ビットの場合）

3.4.1.2.3　AES 暗号（鍵長 256 ビットの場合）



注1　ADD, Sub, Shift, Mix, KRは、基本関数とし3.4.1.2.3.1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3.4.1.2.3.2 に示す。

図 3.4.1.2.3-1　AES 暗号のアルゴリズム（鍵長 256 ビットの場合）

3.4.1.2.3.1　基本関数

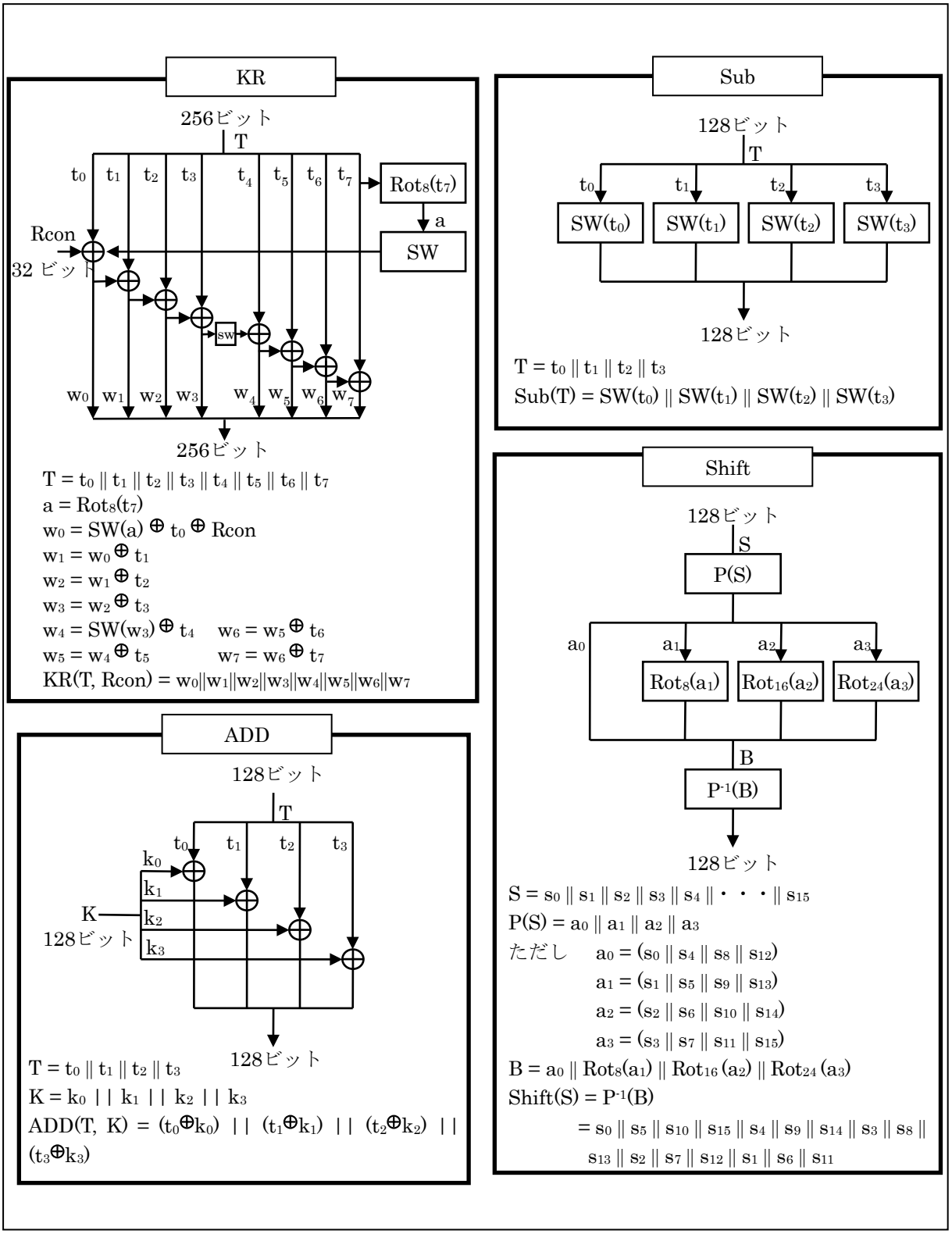


図 3.4.1.2.3.1-1　AES 暗号の基本関数（鍵長 256 ビットの場合）

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3.4.1.2.3.2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。

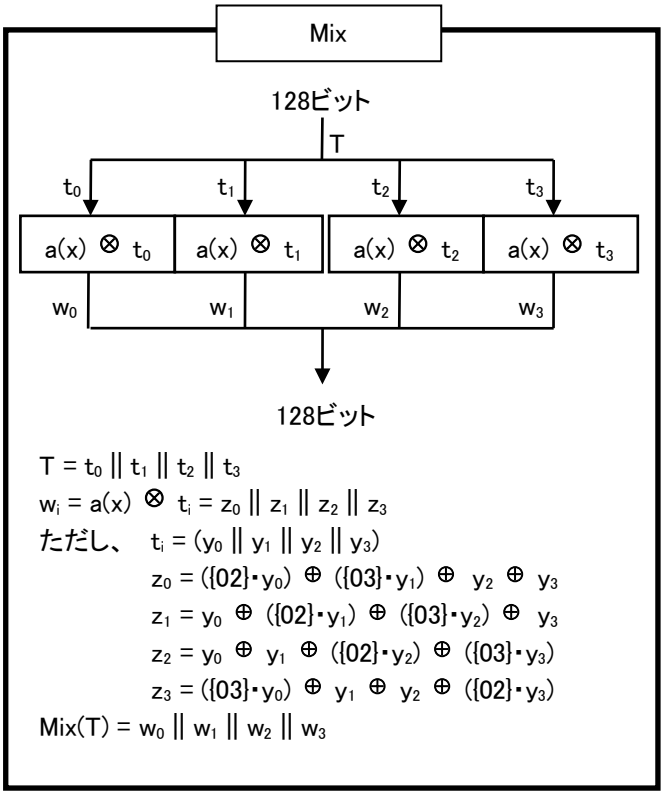


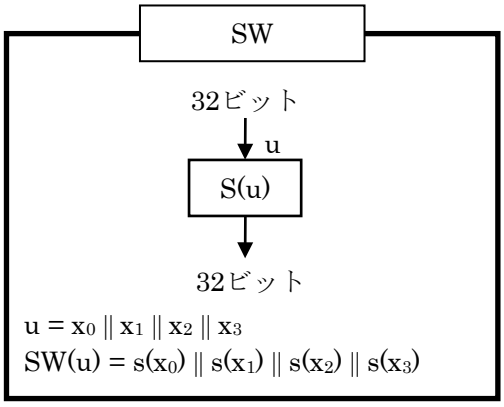
図 3.4.1.2.3.1-2　AES 暗号の基本関数（鍵長 256 ビットの場合）

3.4.1.2.3.2　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
注　数値は16進表記とする。

補助関数



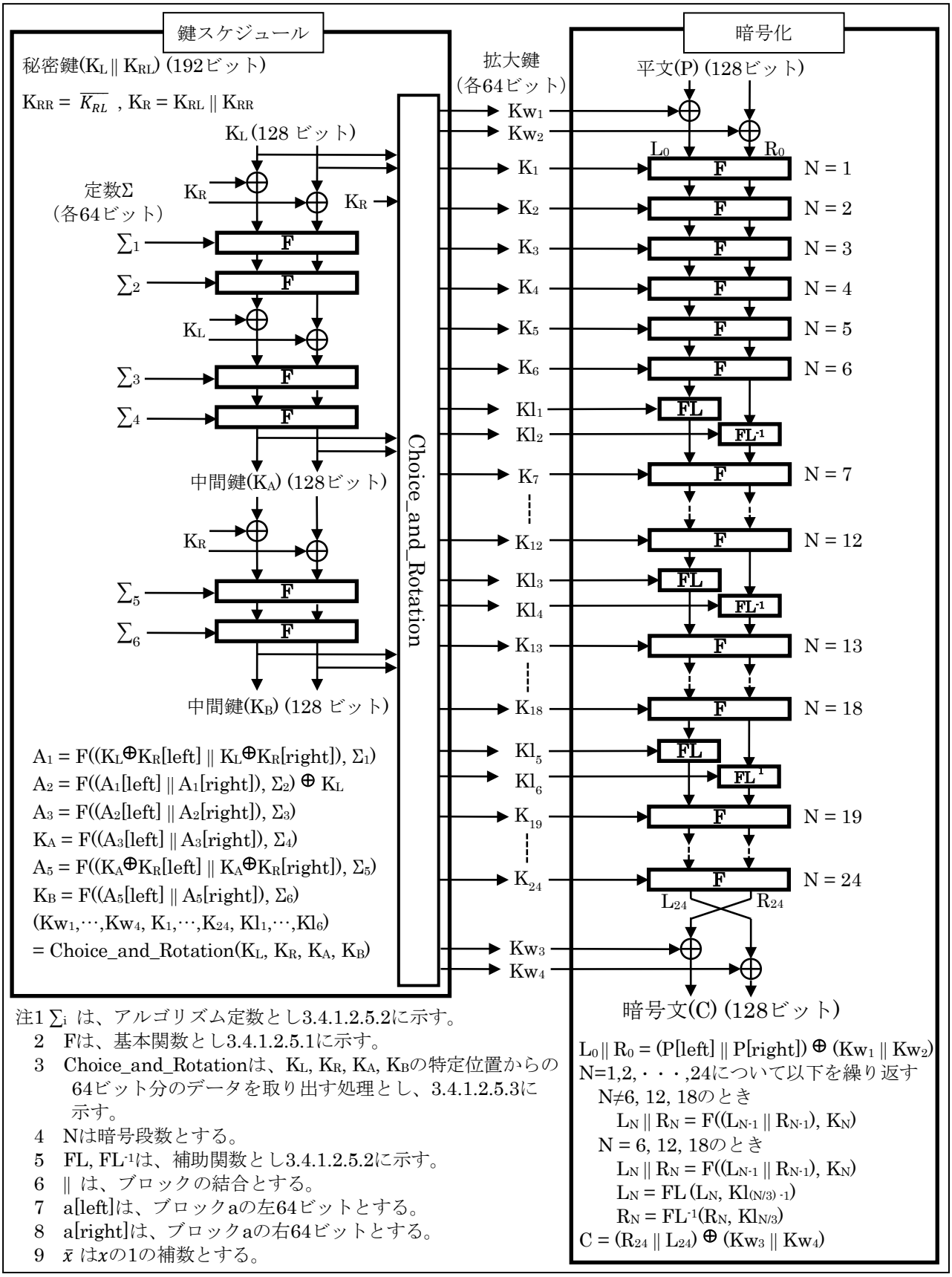
注1　u は、補助関数への入力とする。
　2　‖ は、ブロックの結合とする。
　3　s は、8ビットの置換表とし、詳細は ISO/IEC 18033-3 に従うものとする。

図 3.4.1.2.3.2-1　AES 暗号のアルゴリズム定数と補助関数（鍵長 256 ビットの場合）

3.4.1.2.4　Camellia 暗号（鍵長 128 ビットの場合）

鍵長 128 ビットの場合の Camellia 暗号は、平成 26 年総務省告示第 235 号別表第三号別記第 1～別記第 5 に基づくものとする。

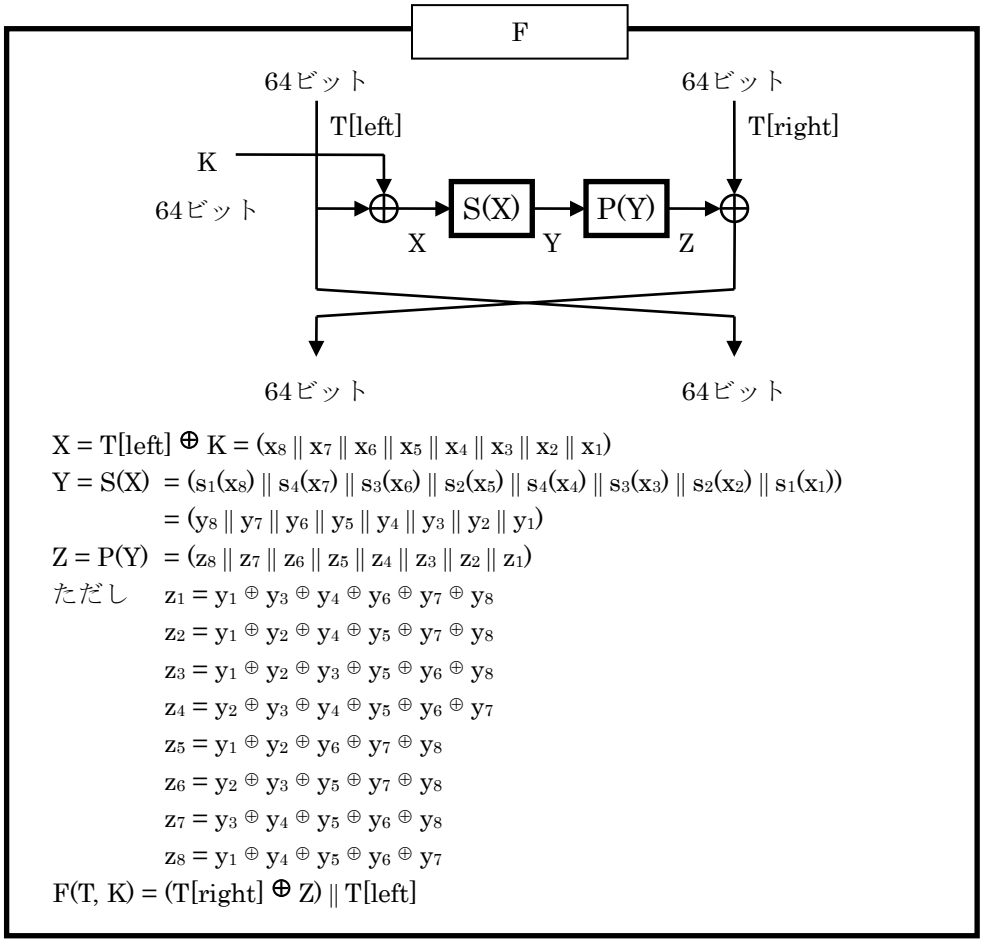
3.4.1.2.5　Camellia 暗号（鍵長 192 ビットの場合）



注1 $\sum_i$ は、アルゴリズム定数とし3.4.1.2.5.2に示す。
2　Fは、基本関数とし3.4.1.2.5.1に示す。
3　Choice_and_Rotationは、KL, KR, KA, KB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、3.4.1.2.5.3に示す。
4　Nは暗号段数とする。
5　FL, FL-1は、補助関数とし3.4.1.2.5.2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。
9　$\bar{x}$ はxの1の補数とする。

図 3.4.1.2.5-1　Camellia 暗号のアルゴリズム（鍵長 192 ビットの場合）

3.4.1.2.5.1　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

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

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

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

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

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

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

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

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

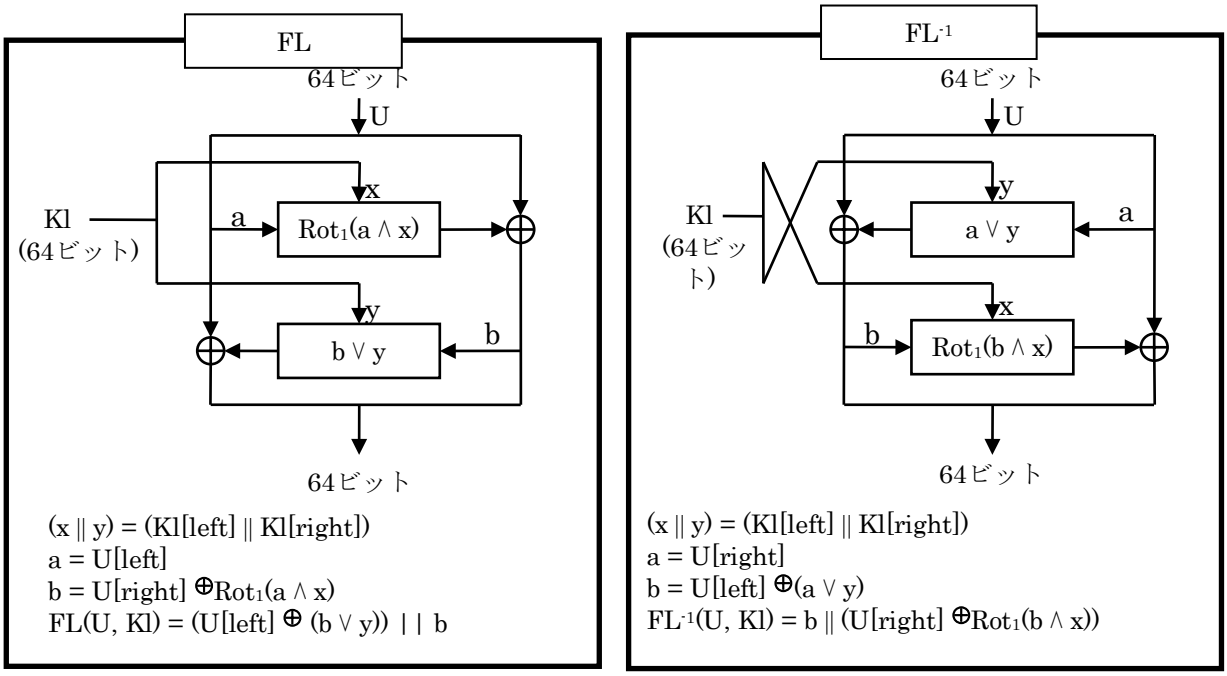
$F(T, K) = (T[right] \oplus Z) \| T[left]$

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 3.4.1.2.5.1-1　Camellia 暗号の基本関数

3.4.1.2.5.2　補助関数とアルゴリズム定数補助関数とアルゴリズム定数

補助関数



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　Rot_1 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

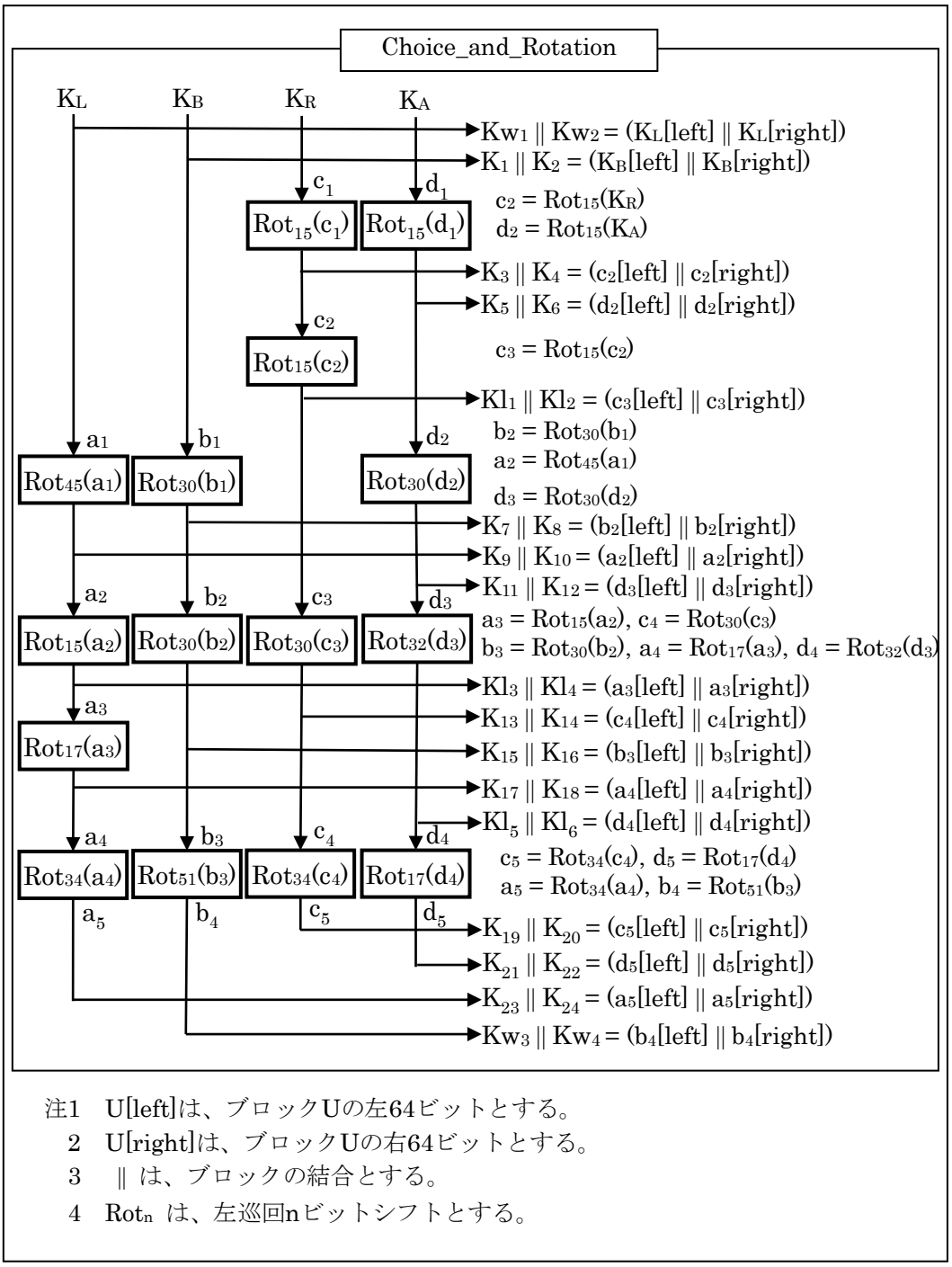
Σ_5 = 10e527fade682d1d

Σ_6 = b05688c2b3e6c1fd

注　数値は16進表記とする。

図 3.4.1.2.5.2-1　Camellia 暗号の補助関数とアルゴリズム定数

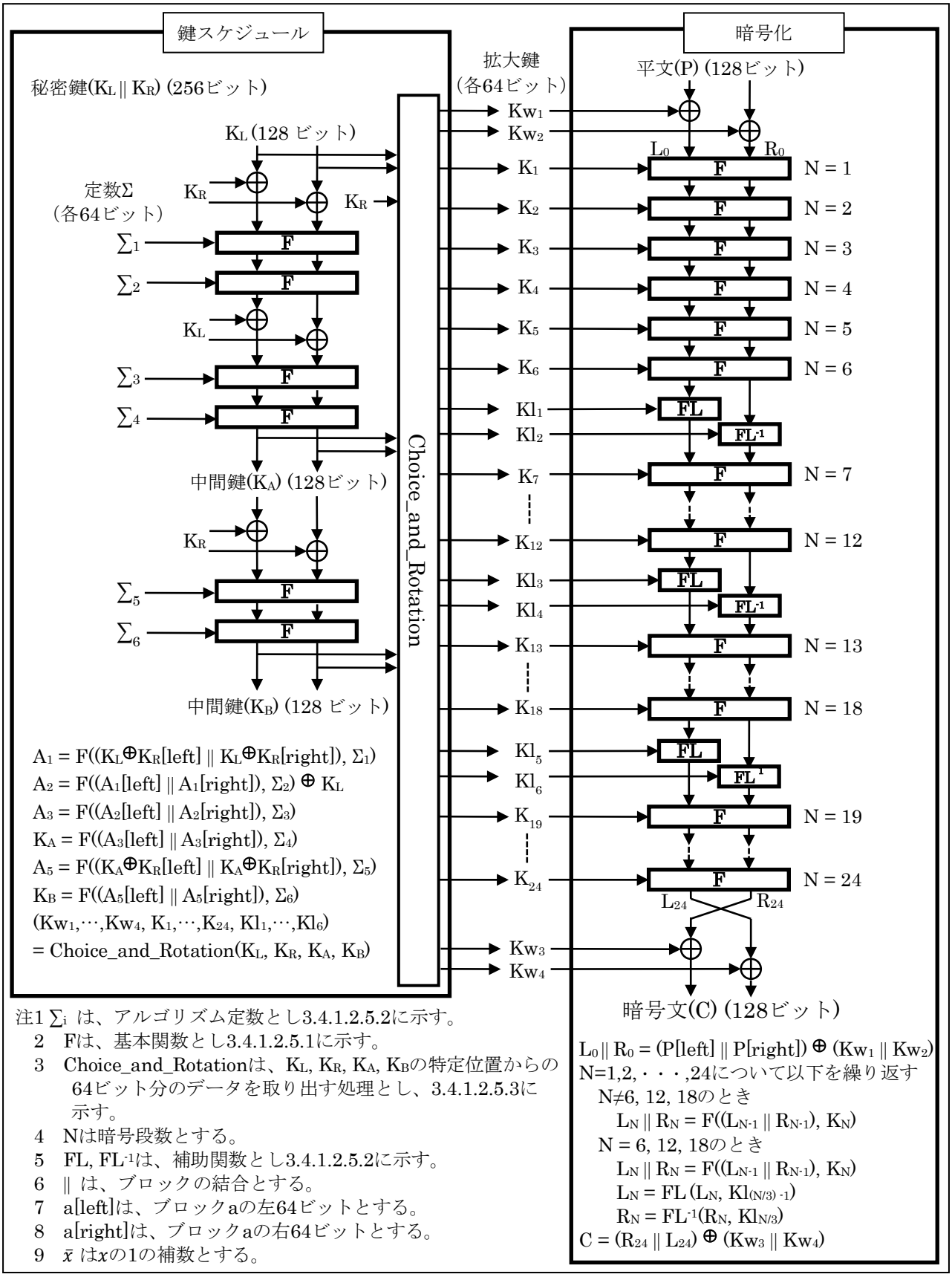
3.4.1.2.5.3　Choice_and_Rotation



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　Rotn は、左巡回nビットシフトとする。

図 3.4.1.2.5.3-1　Camellia 暗号の Choice_and_Rotation

3.4.1.2.6　Camellia 暗号（鍵長 256 ビットの場合）



注1 $\sum_i$ は、アルゴリズム定数とし3.4.1.2.5.2に示す。
2　Fは、基本関数とし3.4.1.2.5.1に示す。
3　Choice_and_Rotationは、KL, KR, KA, KB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、3.4.1.2.5.3に示す。
4　Nは暗号段数とする。
5　FL, FL-1は、補助関数とし3.4.1.2.5.2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。
9　$\bar{x}$ はxの1の補数とする。

図 3.4.1.2.6-1　Camellia 暗号のアルゴリズム（鍵長 256 ビットの場合）

3.4.1.3　スクランブル手順

スクランブル手順に関して、暗号利用モードはCTRモードまたはCBCモードとする

（理由）

現行方式（4K8K衛星放送）との整合性、及びCENCの規定との整合性を確保するため。

3.4.1.3.1　AESを用いたスクランブル手順（CTRモード）

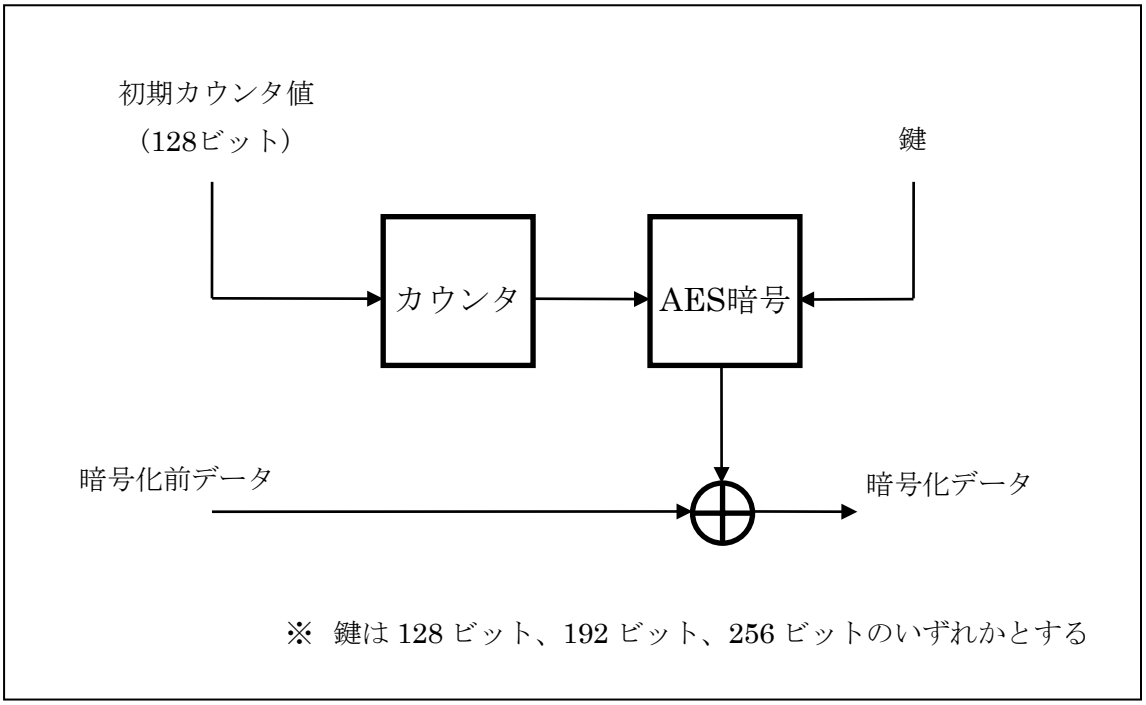


図3.4.1.3.1-1　AESを用いたスクランブル手順（CTRモード）

3.4.1.3.2　AESを用いたスクランブル手順（CBCモード）

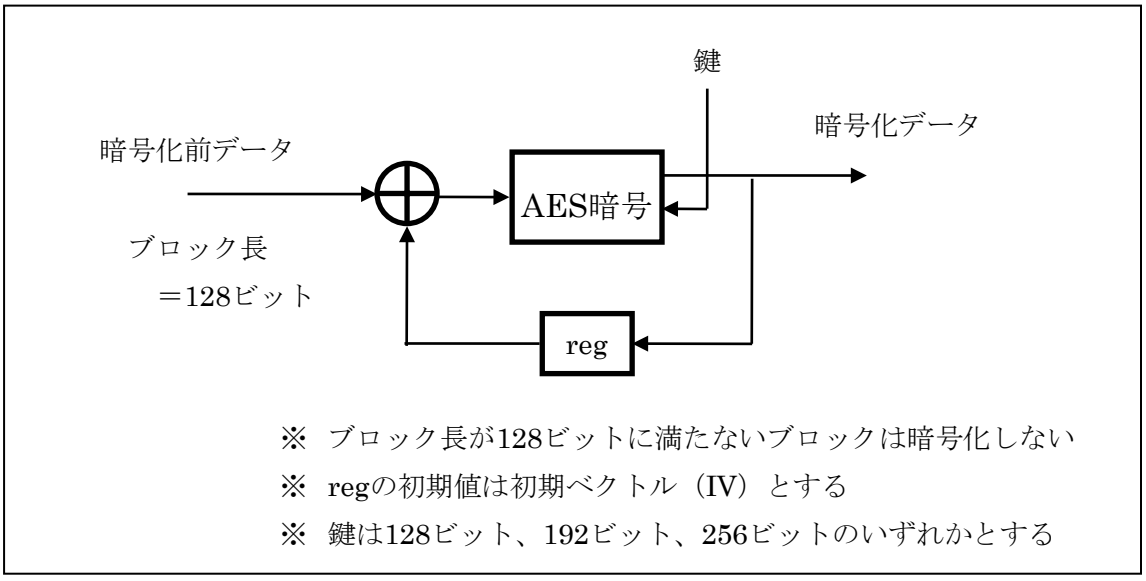


図3.4.1.3.2-1　AESを用いたスクランブル手順（CBCモード）

3.4.1.3.3　Camellia を用いたスクランブル手順（CTR モード）

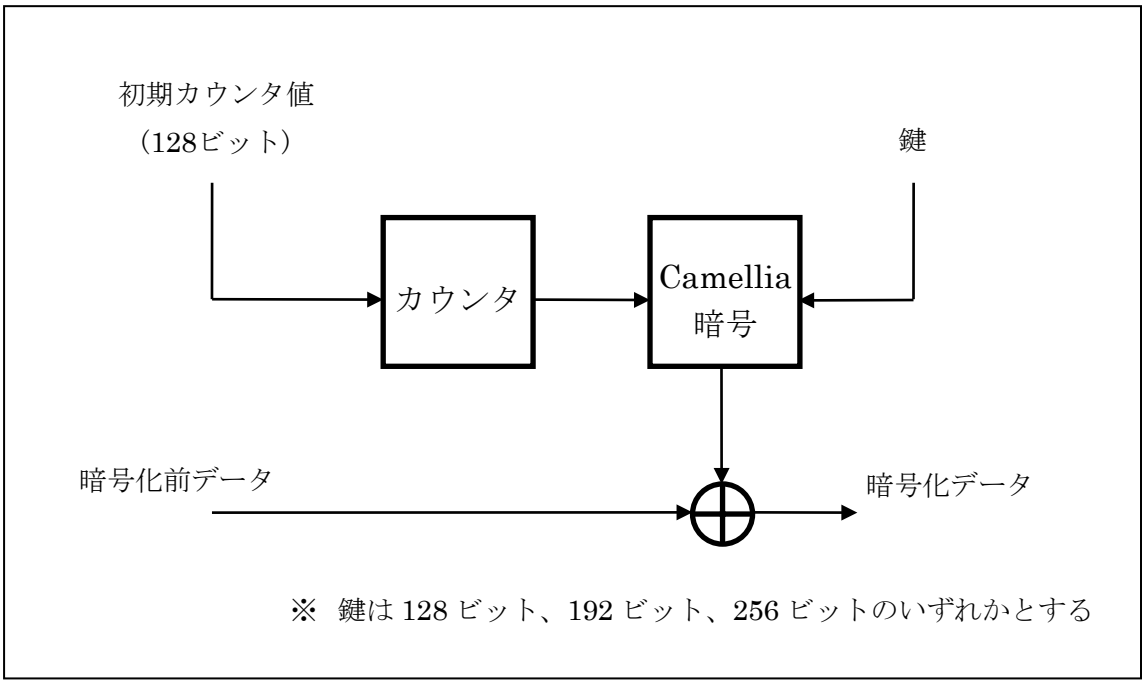


図 3.4.1.3.3-1　Camellia を用いたスクランブル手順（CTR モード）

3.4.1.3.4　Camellia を用いたスクランブル手順（CBC モード）

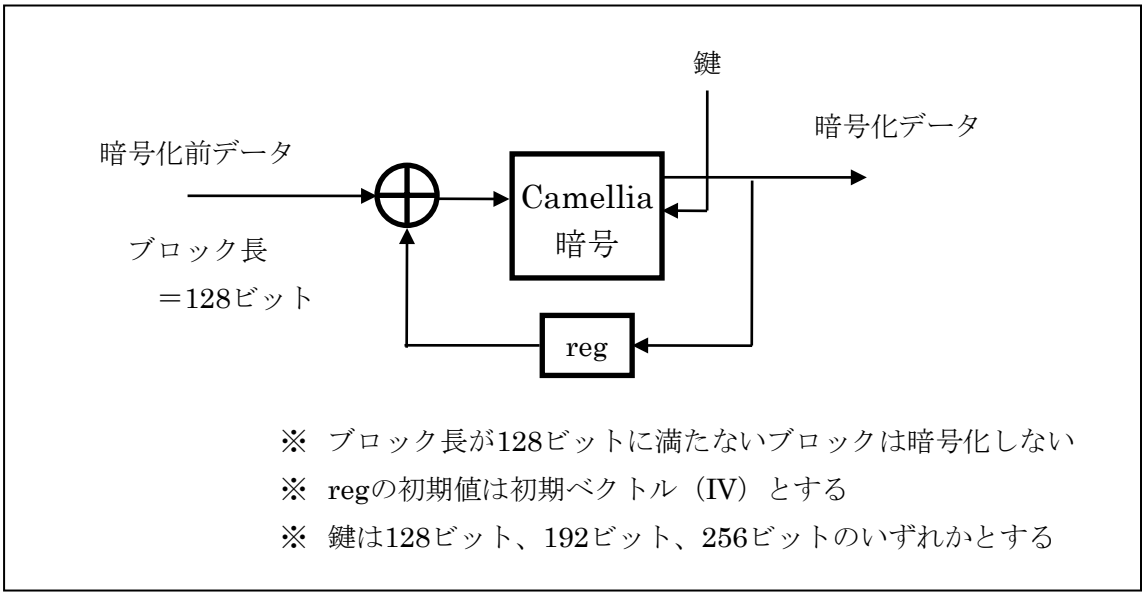


図 3.4.1.3.4-1　Camellia を用いたスクランブル手順（CBC モード）

3.4.1.4　スクランブルの範囲

スクランブルの範囲は、MMTP パケットのペイロード部のデータ部（全部もしくはその一部）及び IP パケットのペイロード部とする。

（理由）

現行方式（4K8K 衛星放送）との整合性、及び CENC の規定との整合性を確保するため。

現行方式（4K8K 衛星放送）との整合性を確保するため、スクランブルの範囲は MMTP パケットのペイロード部のデータ部及び IP パケットのペイロード部とする。ただし、CENC の場合はデータ部の全てではなく、その一部を暗号化する仕様があり、CENC の規定との整合性を確保するため、データ部の一部を暗号化することも可能とする。

3.4.1.5　スクランブル方式に係る伝送制御信号

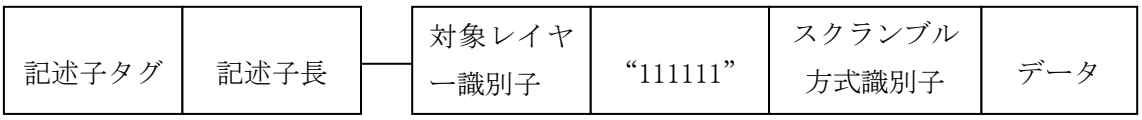
現行方式（4K8K 衛星放送）と同様、スクランブルサブシステムの識別のために、平成 26 年総務省告示第 233 号別表第 29 号に記載の伝送制御信号（CA メッセージ）に配置される CA テーブル（平成 26 年総務省告示第 233 号別表第 29 号別記）に配置可能な記述子として、スクランブル方式記述子（図 3.4.1.5-1）を導入する。スクランブル方式記述子の構成は平成 26 年総務省告示第 233 号別表第 30 号別記第 4 と同じであるが、鍵長 128 ビット、192 ビット、256 ビットのいずれかを選択できるようにするため、スクランブル方式識別子の値を追加した（表 3.4.1.5-1）。

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）について検討するとともに、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を検討した。ただし、メッセージ認証方式記述子が配置されない場合は、メッセージ認証を行わない（メッセージ認証コードが付加されない）ことを示す。なお、放送で映像音声のコンポーネントを配信し、通信で字幕データ等のコンポーネントを配信するケースも想定されるが、通信で配信されるコンポーネントに関しては、コンテンツ保護のために、各種 DRM などを適用することも想定される。この場合、必要に応じて、各記述子の拡張領域に各種 DRM に関するセキュリティ情報を記述することも想定されるが、その詳細は、事業者任意規格とする。

なお、メッセージ認証方式記述子に関しては、放送番組を受信するために必須な仕組みではないことから、民間規格として定めることが適当である。

（理由）

スクランブル方式に脆弱性が発見された場合において対応可能とするため。



注 1）記述子タグの値は、スクランブル方式記述子を示す 0x8005 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（表 3.4.1.5-1）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 3.4.1.5-1：スクランブル方式記述子の構成

表 3.4.1.5-1：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	AES、鍵長 192 ビット
00000100	Camellia、鍵長 192 ビット
00000101	AES、鍵長 256 ビット
00000110	Camellia、鍵長 256 ビット
00000111 - 11111111	未定義

5　今後の課題

5.1　限定受信方式

① スクランブル方式の暗号アルゴリズムや鍵長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、及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。
- 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。

② 鍵の更新頻度については、民間規格や運用検討の場において議論・検討する必要がある。その際、以下の各項に留意することが望ましい。

- 4K8K 衛星放送と同様のスクランブル方式を用いる場合、現行の鍵更新頻度で良いかどうか議論する必要がある。
- スクランブル方式に CENC を用いる場合、鍵を取得する際に受信機と DRM ライセンスサーバ間の通信が発生するため、現行の鍵更新頻度よりも少なくする必要がある。
- 鍵長と鍵更新頻度はトレードオフの関係にあるため、鍵長の選択とセットで考える必要がある。

③ 関連情報サブシステムに関しては、現状を維持しつつ、高度地上デジタルテレビジョン放送方式におけるサービス要件が決まり次第、民間規格や運用検討の場において議論・検討する必要がある。

④ 多重化方式の検討にあたって、Web ブラウザによる提示を想定する以下の 3 種類のシステムモデルが想定されている。受信機におけるスクランブルサブシステムの責任分界点をどこに設定するのか、民間規格や運用検討の場において議論・検討する必要がある。

- CMAF を用いない場合（現行の 4K8K 衛星放送と同様）
- 受信機システムで CMAF 形式に変換し、ブラウザで提示する場合
- 放送事業者から CMAF 形式で信号を送出し、受信機システムのブラウザに直接入力する場合

参考資料１　要求条件との適合性

◆システム

項目	要求条件	適合性
著作権保護	放送及び通信コンテンツの視聴者による記録等を制御できる機能を有すること	高度地上デジタルテレビジョン放送方式におけるサービス要件が明確化したのち検討する必要がある
個人情報保護	受信者の個人情報保護について考慮すること	現行の地上デジタル放送や4K8K衛星放送と同等の機能を実現可能である
サイバーセキュリティ	放送及び通信コンテンツの送出並びに送信装置へのサイバー攻撃に対する防御について考慮すること	現行の地上デジタル放送や4K8K衛星放送と同じく、放送局が適切な防御策を講じることにより実現可能である

◆技術方式

項目		要求条件	適合性
コンテンツ保護	スクランブルサブシステム	高度な秘匿性を有すること	・　AESブロック暗号とCamelliaブロック暗号を選択可能とした ・　スクランブル方式に脆弱性が発見された場合において対応可能とするために、送信側でスクランブル方式の暗号アルゴリズムを指定できる仕組みを導入した
		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	
コンテンツ保護	関連情報サブシステム	関連情報伝送やコンテンツ保護に関して十分な安全性を有し、その安全性を継続的に維持・改善できること	高度地上デジタルテレビジョン放送方式におけるサービス要件が明確化したのち検討する必要がある
		種々のサービス形態に対応するため、課金・収納方式等に自由度があり、 弾力的な運用できること	
		個々の受信者へ向けた情報の伝送・表示ができること	

		新規関連情報サブシステムへの更新や拡張性を考慮すること	
		関連情報はできるだけ共通の形式によること	
		関連情報の配付は、効率的で正確、確実なものであること	

◆受信機

項目	要求条件	適合性
共通性／ インターフェース	適切なコンテンツ保護を実現する機能を有すること	民間規格及び受信機設計において考慮されることを想定した
動作	個人情報を保護する機能を有すること	民間規格及び受信機設計において考慮されることを想定した
サイバーセキュリティ	受信機へのサイバー攻撃に対する防御について考慮すること	民間規格及び受信機設計において考慮されることを想定した