■1 群（信号・システム）- 3 編（暗号理論）

3 章 暗号利用モード

（執筆者：岩田　哲）[2018 年 12 月 受領]

■概要■

ブロック暗号を用いることで，ある固定のブロック長の平文を暗号化できるが，これ自体では任意の長さの平文を暗号化することはできない．一方で，暗号化する平文は様々な長さを取りうる．

ブロック暗号利用モードは，ブロック暗号を構成要素として用いて，実用に即した様々な機能を実現するためのアルゴリズムである．平文の暗号化のためのブロック暗号利用モードを暗号化モードといい，これを用いることで任意の長さの平文を暗号化できる．通信路上のデータの改ざんや，あるいは成りすましを検出するためのメッセージ認証は暗号化とともに，安全な通信の実現には欠かせない機能であり，メッセージ認証コードを用いることでこれを実現できる．

本章では，代表的な暗号化モードとメッセージ認証のためのブロック暗号利用モード（メッセージ認証コード）を紹介する．また，暗号化とメッセージ認証を同時に，そして効率的に行うことができる認証暗号化のためのブロック暗号利用モード（認証暗号化モード）についても紹介する．

【本章の構成】

3-1 章では暗号化モードを取り上げ，ECB モード，CBC モード，CTR モードを紹介する．3-2 章ではメッセージ認証コードを紹介し，CMAC を紹介する．3-3 章では認証暗号化モードを取り上げ，GCM の概略を紹介する．

■1 群 - 3 編 - 3 章

3-1 暗号化モード

（執筆者：岩田　哲）[2018 年 12 月 受領]

ブロック暗号利用モードは，ブロック暗号を構成要素として用いて，様々な機能を実現するためのアルゴリズムである．任意の長さの平文を暗号化するためのブロック暗号利用モードを暗号化モードという．数多くの暗号化モードが知られており，本章では，NIST Special Publication 800-38A [9] に記載されている代表的な暗号化モードである ECB モード，CBC モード，CTR モードを紹介する．

ブロック長が n ビット，秘密鍵が K であるブロック暗号の暗号化関数を $E_K(\cdot)$ と書き，$C = E_K(M)$ により，平文 M に対する暗号文 C を表す．M と C はともに n ビットであり，K のビット長は使用するブロック暗号に依存する．例えば AES であれば $n = 128$ であり，秘密鍵のビット長は 128，192，256 ビットのいずれかである．ブロック暗号の暗号化関数 $E_K(\cdot)$ は，各秘密鍵 K に対して n ビット上の置換であるから，その逆関数が存在し，これを $D_K(\cdot)$ と書く．これはブロック暗号の復号関数であり，$M = D_K(C)$ は，暗号文 C を復号した結果が平文 M であることを表す．なお任意の平文 M と任意の秘密鍵 K に対し，$D_K(E_K(M)) = M$ が成り立つ．

3-1-1 ECB モード

ECB モード（Electronic Codebook Mode）はもっとも素朴な暗号化モードであり，平文 M を n ビットごとに分割し，各平文ブロックを独立にブロック暗号を用いて暗号化する．

具体的には，M を暗号化する平文とし，これを n ビットごとに $M = (M[1],\ldots,M[m])$ と分割する．ECB モードでは平文のビット長は n の倍数でなければならず，ここでは M は全部で m ブロックからなるとする．各 $M[i]$ は n ビットである．ECB モードの暗号化は次の式によって定義される．

$$C[i] = E_K(M[i]) \text{ for } i = 1,\ldots,m$$

暗号文は $C = (C[1],\ldots,C[m])$ である．

復号は暗号文 $C = (C[1],\ldots,C[m])$ に対して，次のように定義される．

$$M[i] = D_K(C[i]) \text{ for } i = 1,\ldots,m$$

この式より平文 $M = (M[1],\ldots,M[m])$ を得る．$m = 3$ の場合の暗号化と復号の例を図 3･1 に示す．

ECB モードにおける暗号化ではブロック暗号の暗号化関数の並列実行が可能である．同様に，ECB モードにおける復号でもブロック暗号の復号関数の並列実行が可能である．

安全性に関して，ECB モードの暗号化では，ブロック暗号の暗号化関数が n ビット上の置換であることから，同じ平文ブロックは同じ暗号文ブロックに暗号化され，異なる平文ブロックは異なる暗号文ブロックに暗号化される．つまり $M[i] = M[j] \Leftrightarrow C[i] = C[j]$ という関係式が成り立ち，ECB モードの暗号文からは，平文に関する部分情報が漏えいする．このことが問題になるような場合は ECB モードを利用することはできない．

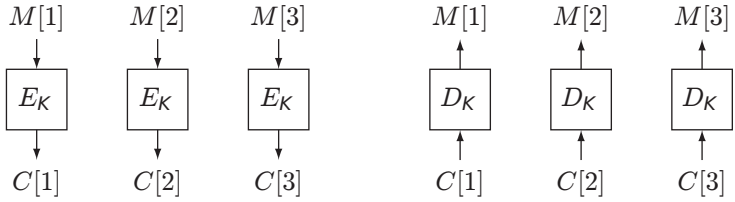

図 3･1 ECB **モードによる暗号化（左図）と復号（右図）.**

3-1-2 CBC モード

CBC モード（Cipher Block Chaining Mode）では，平文ブロックと直前の暗号文ブロックを排他的論理和により組み合わせて暗号化を行う．また，平文の 1 ブロック目の暗号化の際には初期値 IV を用いる．IV は n ビットのデータであり，秘密である必要はないが予測不可能な値でなければならない．また復号に必要なため，何らかの方法で受信者と共有する必要がある．

ECB モードと同様に，CBC モードでは平文 M のビット長は n の倍数でなければならず，これを n ビットごとに $M=(M[1],\ldots,M[m])$ と分割する．CBC モードの暗号化は次式によって定義される．

$$C[i]=\begin{cases} E_K(M[1]\oplus IV) & \text{for } i=1 \\ E_K(M[i]\oplus C[i-1]) & \text{for } i=2,\ldots,m \end{cases}$$

暗号文は $C=(C[1],\ldots,C[m])$ である．なお IV を暗号文に含めてもよい．また，$X\oplus Y$ はビット列 X と Y のビットごとの排他的論理和を表す．

復号は初期値 IV と暗号文 $C=(C[1],\ldots,C[m])$ に対して，次のように定義される．

$$M[i]=\begin{cases} D_K(C[1])\oplus IV & \text{for } i=1 \\ D_K(C[i])\oplus C[i-1] & \text{for } i=2,\ldots,m \end{cases}$$

この式より平文 $M=(M[1],\ldots,M[m])$ を得る．$m=3$ の場合の暗号化と復号の例を図 3･2 に示す．

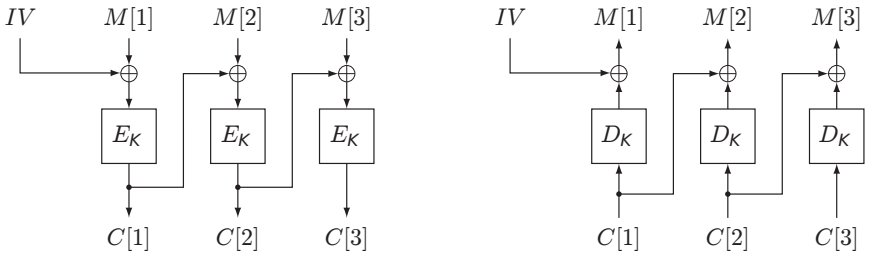

図 3･2 CBC **モードによる暗号化（左図）と復号（右図）.**

CBC モードにおける暗号化では，$C[i-1]$ の値を $M[i]$ を暗号化する際に用いるため，ブロック暗号の暗号化関数を並列に実行することはできない．一方で，CBC モードにおける復号ではブロック暗号の復号関数の並列実行が可能である．

選択平文攻撃によりランダム置換と効率的に識別できないようなブロック暗号を擬似ランダム置換という[22]．CBC モードの安全性に関して，ブロック暗号が擬似ランダム置換であるという仮定のもと，CBC モードが安全な暗号化モードであることが証明されている[2]．

3-1-3 CTR モード

CTR モード（Counter Mode）は，送受信者間で共有したカウンタを用いることにより，暗号化でも復号でもブロック暗号の復号関数を利用しないという特徴を有する．CTR モードではカウンタ系列 $\mathrm{ctr}_1, \mathrm{ctr}_2, \ldots$ を生成し，これらをブロック暗号の暗号化関数で暗号化することにより鍵系列 $S[1], S[2], \ldots$ を生成する．鍵系列と平文の排他的論理和により暗号文を計算する．

CTR モードの暗号化においてカウンタの値が繰り返すと安全性が損なわれるため，同じカウンタの値を使用することはできない．これは一つの平文の暗号化のみならず，その秘密鍵で暗号化するすべての平文に渡って，カウンタの値が繰り返してはならないことを意味する．カウンタ系列は秘密である必要はなく，予測不可能な値である必要もないが，復号に必要なため受信者と共有する必要がある．

ECB モードや CBC モードと異なり, CTR モードでは任意のビット長の平文を暗号化できる．まず平文 M を n ビットごとに $M = (M[1], \ldots, M[m])$ と分割する．ただし，$M[1], \ldots, M[m-1]$ は n ビットであり，最後の $M[m]$ は ℓ ビットであり，$\ell \leq n$ とする．

CTR モードの暗号化は次のように定義される．まずカウンタ系列 $\mathrm{ctr}_1, \mathrm{ctr}_2, \ldots$ より

$$S[i] = E_K(\mathrm{ctr}_i) \text{ for } i = 1, \ldots, m \tag{3・1}$$

として鍵系列 $S[1], \ldots, S[m]$ を生成し，次に

$$C[i] = \begin{cases} S[i] \oplus M[i] & \text{for } i = 1, \ldots, m-1 \\ \mathrm{msb}_\ell(S[m]) \oplus M[m] & \text{for } i = m \end{cases}$$

とする．暗号文は $C = (C[1], \ldots, C[m])$ である．ただし，$\mathrm{msb}_\ell(X)$ は n ビット列 X の上位 ℓ ビットを表す．

復号はカウンタ系列 $\mathrm{ctr}_1, \mathrm{ctr}_2, \ldots$ と暗号文 $C = (C[1], \ldots, C[m])$ に対して，式 (3・1) により鍵系列 $S[1], \ldots, S[m]$ を生成し，次に

$$M[i] = \begin{cases} S[i] \oplus C[i] & \text{for } i = 1, \ldots, m-1 \\ \mathrm{msb}_\ell(S[m]) \oplus C[m] & \text{for } i = m \end{cases}$$

により平文 $M = (M[1], \ldots, M[m])$ を得る．$m = 3$ の場合の暗号化と復号の例を図 3・2 に示す．

CTR モードでは，暗号化でも復号でもブロック暗号の並列実行が可能であり，いずれの場合もブロック暗号の復号関数は使用しない．また，カウンタ系列があれば（平文が未知であっ

ても），ブロック暗号を実行することができる．

安全性に関して，ブロック暗号が擬似ランダム置換であるという仮定のもと，CTR モードが安全な暗号化モードであることが証明されている[2)]．なお CTR モードはブロック暗号を用いたストリーム暗号の構成の一例とみなすことができる．

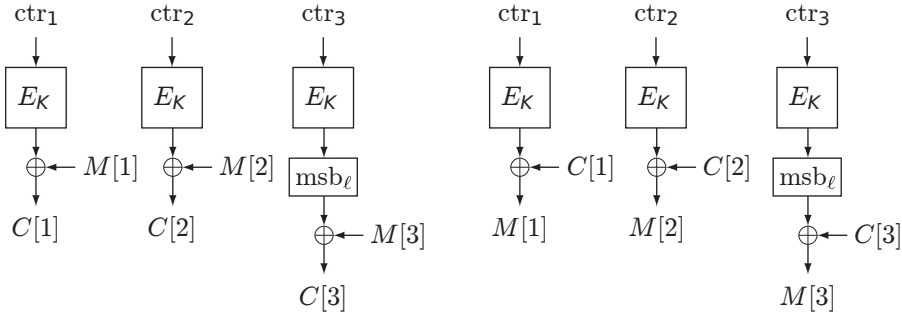

図 3·3　CTR モードによる暗号化（左図）と復号（右図）．

3-1-4 その他の暗号化モード

上記で紹介した以外に，NIST Special Publication 800-38A には CFB モード（Cipher Feedback Mode）と OFB モード（Output Feedback Mode）が記載されている[9)]．また，CBC モードを任意の長さの平文を暗号化できるように一般化した CBC-CS モード（CBC Ciphertext Stealing Mode）が知られている[13)]．

■1 群 - 3 編 - 3 章

3-2 メッセージ認証コード

（執筆者：岩田　哲）[2018 年 12 月 受領]

適切な暗号化モードを用いることで，平文を暗号化して，送受信することができる．一方で，通信路上のデータの改ざんや，あるいは成りすましを検出するためのメッセージ認証は安全な通信の実現には欠かせない機能である．これは暗号化とは本質的に異なる機能であり，一般に暗号化モードでは達成できない．本章では，メッセージ認証のためのブロック暗号利用モードであるメッセージ認証コードとして，NIST Special Publication 800-38B [11] に記載されている CMAC を紹介する．これは Iwata と Kurosawa が提案した OMAC [15] と同一のアルゴリズムであり，ISO/IEC 9797-1:2011 で規定されている CBC-MAC [14]，その改良である XCBC [8] と TMAC [21] を改良した方式である．

3-2-1 CMAC

CMAC（Cipher-based Message Authentication Code）は，ブロック暗号を構成要素として用い，秘密鍵と任意長のメッセージを入力し，固定長のタグを出力する．

$E_K(\cdot)$ により秘密鍵 K を用いたブロック暗号の暗号化関数を表し，そのブロック長を n ビットする．CMAC の秘密鍵は K であり，まず次の手順によりサブ鍵 K_1, K_2 を生成する．

1. $L = E_K(0^n)$
2. $K_1 = \begin{cases} L \ll 1 & \text{if } \mathrm{msb}_1(L) = 0 \\ (L \ll 1) \oplus \mathrm{Cst}_n & \text{else} \end{cases}$
3. $K_2 = \begin{cases} K_1 \ll 1 & \text{if } \mathrm{msb}_1(K_1) = 0 \\ (K_1 \ll 1) \oplus \mathrm{Cst}_n & \text{else} \end{cases}$

ただし，0^n はビット 0 からなる n ビットのビット列 $0\cdots0$ を表す．また，$X \ll 1$ は n ビットのビット列 X の 1 ビット左シフトを表し（$X = (x_1, \ldots, x_n)$ であれば，$X \ll 1 = (x_2, \ldots, x_n, 0)$ である），$\mathrm{msb}_1(X)$ は X の最上位 1 ビットを表す．Cst_n は n に依存する定数であり，$n = 128$ であれば $\mathrm{Cst}_{128} = 0^{120}10000111$ である．なお $n = 128$ の場合，K_1 はガロア体 $\mathrm{GF}(2^{128})$ 上で，規約多項式 $x^{128} + x^7 + x^2 + x + 1$ を法として，L と x との乗算になっている．同様に，K_2 は K_1 と x との乗算である．サブ鍵生成は秘密鍵があればメッセージがなくとも実行することができる．

次に M をメッセージとし，タグを生成する．まず M を n ビットごとに $M = (M[1], \ldots, M[m-1], M^*[m])$ と分割する．$M[1], \ldots, M[m-1]$ は n ビットであり，$M^*[m]$ は ℓ ビット（$\ell \le n$）である．次に，$M[m]$ を

$$M[m] = \begin{cases} M^*[m] \oplus K_1 & \text{if } |M^*[m]| = n \\ (M^*[m]10^{n-1-|M^*[m]|}) \oplus K_2 & \text{else} \end{cases}$$

とする．ただし，XY はビット列 X と Y の連結を表し，$|X|$ は X のビット長を表す．$(M[1], \ldots, M[m])$

に対し，次の手順でタグ T を生成する．

1. $Y[0] = 0^n$
2. $Y[i] = E_K(Y[i-1] \oplus M[i])$ for $i = 1, \ldots, m$
3. $T = \mathrm{msb}_\tau(Y[m])$

ただし，τ はタグのビット長を表す．$m = 3$ の場合のタグ生成の例を図 3･4 に示す．

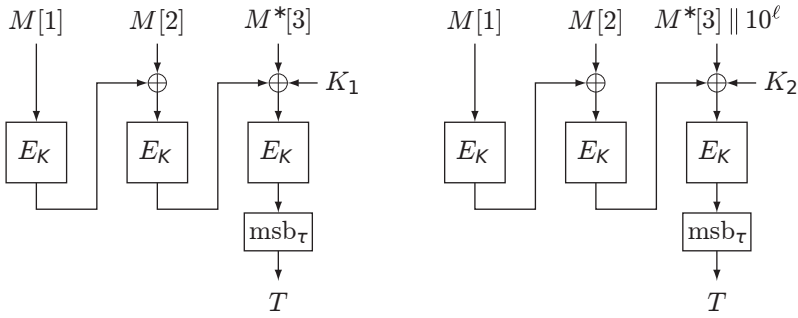

図 3･4　CMAC によるタグ生成．$|M^*[3]| = n$ の場合（左図）と $|M^*[3]| < n$ の場合（右図）．右図において，$\ell = n - 1 - |M^*[3]|$ である．

秘密鍵 K とメッセージ M に対するタグを $T = \mathrm{CMAC}_K(M)$ と書く．CMAC を利用する場合，送受信者間で秘密鍵 K が共有されており，送信者がメッセージ M を送信する際に $T = \mathrm{CMAC}_K(M)$ を計算し，(M,T) を受信者に送信する．受信者が (M',T') を受信したとする．これは送信者が送信した (M,T) をそのまま受信したか，もしくは改ざんや成りすましの可能性があり，受信者はまず $\mathrm{CMAC}_K(M')$ を所有する秘密鍵 K と受信した M' から計算し，$T' = \mathrm{CMAC}_K(M')$ が成り立てばこれを受理する．そうでなければ (M',T') を拒否することによって，改ざんや成りすましを検出できる．

CMAC ではブロック暗号の並列実行はできない．安全性に関して，ブロック暗号が擬似ランダム置換であるという仮定のもと，CMAC が擬似ランダム関数であることが証明されている[15]．また，擬似ランダム関数は安全なメッセージ認証コードであることが証明されている[3]．

3-2-2 その他のメッセージ認証コード

ブロック暗号に基づくメッセージ認証コードとして，PMAC が知られている[7]．PMAC では，ブロック暗号の並列実行が可能である．

数多くのメッセージ認証コードの構成法が知られており，ブロック暗号以外の構成要素から得られる方式として，鍵付き汎用ハッシュ関数から構成される Wegman-Carter MAC [29] が，鍵付き汎用ハッシュ関数とブロック暗号を組み合わせた GMAC [12]や Poly1305-AES [5]，4 章で紹介するハッシュ関数に基づく HMAC [1, 26]などが知られている．また，NIST Special

Publication 800-185 では暗号学的置換を構成要素とするメッセージ認証コード KMAC [19)]が規定されている.

■1 群 - 3 編 - 3 章

3-3 認証暗号化モード

（執筆者：岩田　哲）[2018 年 12 月 受領]

認証暗号化モードを用いることで，暗号化とメッセージ認証を同時に，かつ効率的に行うことができる．本章では NIST Special Publication 800-38D [12]に記載されている GCM の概略を紹介する．これは，McGrew と Viega により提案された認証暗号化モードである[23]．

3-3-1 GCM

GCM（Galois/Counter Mode）は，ガロア体 GF(2^n) 上の乗算を用いたメッセージ認証コードと，CTR モードを組み合わせることにより，暗号化とメッセージ認証を行う．

$E_K(\cdot)$ をブロック長 n ビット，秘密鍵が K であるブロック暗号の暗号化関数とする．NIST Special Publication 800-38D [12]ではブロック長が 128 ビットのブロック暗号を使用するよう規定されており，以降 $n=128$ とする．GCM では，内部でサブルーチンとして GHASH と GCTR を用いる．GHASH は鍵付き汎用ハッシュ関数であり，128 ビットの秘密鍵 L とビット列 X を入力とし，128 ビットの出力を返す．X のビット長は 128 の倍数であり，$X=(X[1],\ldots,X[x])$ と x ブロックからなる場合，GHASH の出力 $Y[x]$ は次の手順により得られる．

1. $Y[0]=0^{128}$
2. $Y[i]=(Y[i-1]\oplus X[i])\cdot L$ for $i=1,\ldots,x$

ただし，乗算はガロア体 GF(2^{128}) 上で，規約多項式 $1+x+x^2+x^7+x^{128}$ を法とする．$Y[x]=\mathrm{GHASH}_L(X)$ と書く．

GCTR は CTR モードの一例であり，秘密鍵 K，カウンタの初期値 $I[1]$ と平文 M を入力として，暗号文 C を出力する．平文 M を 128 ビットごとに $M=(M[1],\ldots,M[m])$ と分割する．$M[1],\ldots,M[m-1]$ は 128 ビットであり，$M[m]$ は ℓ ビットであり，$\ell\le 128$ とする．カウンタの初期値 $I[1]$ より，カウンタ系列 $I[2],\ldots,I[m]$ を生成する．これは，

$$I[i]=\mathrm{inc}_{32}(I[i-1]) \text{ for } i=2,\ldots,m \tag{3・2}$$

として得られる．ただし，$\mathrm{inc}_{32}(X)$ は X の下位 32 ビットに 1 を算術加算する演算を表す．次に，

$$S[i]=E_K(I[i]) \text{ for } i=1,\ldots,m \tag{3・3}$$

として鍵系列 $S[1],\ldots,S[m]$ を生成し，

$$C[i]=\begin{cases} S[i]\oplus M[i] & \text{for } i=1,\ldots,m-1 \\ \mathrm{msb}_\ell(S[m])\oplus M[m] & \text{for } i=m \end{cases}$$

とする．暗号文は $C=(C[1],\ldots,C[m])$ である．$C=\mathrm{GCTR}_K(I[1],M)$ と書く．

GCTR の復号はカウンタの初期値 $I[1]$ と暗号文 C を入力として，平文 M を出力する．式

(3･2)，式 (3･3) に従い $S[1],\ldots,S[m]$ を生成し，

$$M[i]=\begin{cases} S[i]\oplus C[i] & \text{for } i=1,\ldots,m-1 \\ \mathrm{msb}_\ell(S[m])\oplus C[m] & \text{for } i=m \end{cases}$$

として平文 $M=(M[1],\ldots,M[m])$ を返す．$M=\mathrm{GCTR}_K^{-1}(I[1],C)$ と書く．

GCM の暗号化アルゴリズムは，秘密鍵 K，ナンス N，ヘッダ A，平文 M を入力とし，暗号文 C とタグ T を出力する．ナンスは安全性のために必要なデータであり，GCM の暗号化において繰り返さないことが要求される．ここではナンスが 96 ビットの場合を考える．ヘッダ A は，暗号化はせず，認証のみを行うデータであり，平文 M は暗号化も認証も行うデータである．暗号文 C と平文 M は同じビット長であり，タグ T は固定長の τ ビットであるとする．暗号化アルゴリズムは次のように定義される．

1. $L=E_K(0^n)$
2. $I[0]=N0^{31}1$
3. $C=\mathrm{GCTR}_K(\mathrm{inc}_{32}(I[0]),M)$
4. S を $S=\mathrm{GHASH}_L(A0^vC0^u[|A|]_{64}[|C|]_{64})$ とする．ただし，$v=128\lceil|A|/128\rceil-|A|$ であり，$v=128\lceil|C|/128\rceil-|C|$ とし，$\lceil z\rceil$ は実数 z の小数点以下切り上げを表す．また，$[|A|]_{64}$ と $[|C|]_{64}$ はそれぞれ $|A|$ と $|C|$ の 64 ビットの 2 進数表現を表す．
5. $T=\mathrm{msb}_\tau(E_K(I[0])\oplus S)$
6. (C,T) を出力する．

GCM の復号アルゴリズムは (K,N,A,C,T) を入力とし，平文 M か，あるいは改ざん，成りすましがあったことを示す記号 $\perp$ を出力する．次のように動作する．

1. $L=E_K(0^n)$
2. $I[0]=N0^{31}1$
3. $M=\mathrm{GCTR}_K^{-1}(\mathrm{inc}_{32}(I[0]),C)$
4. S を $S=\mathrm{GHASH}_L(A0^vC0^u[|A|]_{64}[|C|]_{64})$ とする．ただし，$v=128\lceil|A|/128\rceil-|A|$ であり，$v=128\lceil|C|/128\rceil-|C|$ である．
5. $T^*=\mathrm{msb}_\tau(E_K(I[0])\oplus S)$
6. $T=T^*$ であれば M を，そうでなければ $\perp$ を出力する．

GCM の暗号化の概略を図 3･5 に示す．

GCM では，暗号化でも復号でもブロック暗号の並列実行が可能であり，ブロック暗号の

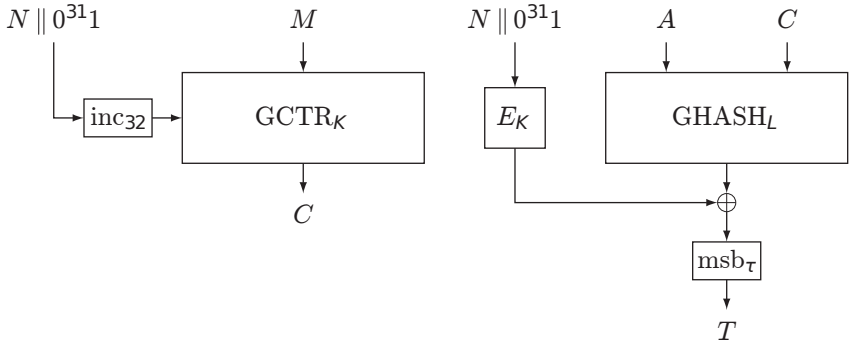

図 3·5　GCM の暗号化の概略．

復号関数は用いない．安全性に関して，暗号化とメッセージ認証両方の意味で安全な認証暗号化モードは，安全な認証暗号化モードである[18, 4]．ブロック暗号が擬似ランダム置換であるという仮定のもと，GCM が安全な認証暗号化モードであることが証明されている[16, 27]．

3-3-2 その他の認証暗号化モード

NIST Special Publication 800-38C [10]では，CCM が規定されている．これは暗号化に CTR モードを，メッセージ認証に CBC-MAC を用いる認証暗号化モードである．IAPM [17]と OCB [28, 20]はいずれもブロック暗号の並列実行が可能で，効率的に動作する認証暗号化モードである．OTR は OCB からブロック暗号の復号関数を取り除くことにより OCB を改良した認証暗号化モードである[24]．

暗号化とメッセージ認証を同時に実現する認証暗号化方式は，ブロック暗号以外からも構成できる．SpongeWrap [6]は暗号学的置換から構成される認証暗号化方式である．また安全な暗号化方式とメッセージ認証コードから，汎用的に認証暗号化方式を構成できることが知られている[4, 25]．

■参考文献

1) Bellare, M., Canetti, R., Krawczyk, H.: Keying Hash Functions for Message Authentication. In: Koblitz, N. (ed.) CRYPTO ’96. LNCS, vol. 1109, pp. 1–15. Springer (1996)
2) Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption. In: FOCS ’97. pp. 394–403. IEEE Computer Society (1997)
3) Bellare, M., Kilian, J., Rogaway, P.: The Security of the Cipher Block Chaining Message Authentication Code. J. Comput. Syst. Sci. 61(3), 362–399 (2000)
4) Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. J. Cryptology 21(4), 469–491 (2008)
5) Bernstein, D.J.: The Poly1305-AES Message-Authentication Code. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 32–49. Springer (2005)
6) Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: Duplexing the Sponge: Single-Pass Authenticated En- cryption and Other Applications. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 320–337. Springer (2011)

7) Black, J., Rogaway, P.: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 384–397. Springer (2002)
8) Black, J., Rogaway, P.: CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. J. Cryp- tology 18(2), 111131 (2005)
9) Dworkin, M.J.: NIST Special Publication 800-38A 2001 Edition. Recommendation for Block Cipher Modes of Operation: Methods and Techniques (2001)
10) Dworkin, M.J.: NIST Special Publication 800-38C. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality (2004)
11) Dworkin, M.J.: NIST Special Publication 800-38B. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication (2005)
12) Dworkin, M.J.: NIST Special Publication 800-38D. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (2007)
13) Dworkin, M.J.: Addendum to NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode (2010)
14) ISO/IEC 9797-1:2011. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher (2011)
15) Iwata, T., Kurosawa, K.: OMAC: One-Key CBC MAC. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 129–153. Springer (2003)
16) Iwata, T., Ohashi, K., Minematsu, K.: Breaking and Repairing GCM Security Proofs. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 31–49. Springer (2012)
17) Jutla, C.S.: Encryption Modes with Almost Free Message Integrity. J. Cryptology 21(4), 547–578 (2008)
18) Katz, J., Yung, M.: Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 284–299. Springer (2000)
19) Kelsey, J., Chang, S., Perlner, R.: NIST Special Publication 800-185. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash (2016)
20) Krovetz, T., Rogaway, P.: The Software Performance of Authenticated-Encryption Modes. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 306–327. Springer (2011)
21) Kurosawa, K., Iwata, T.: TMAC: Two-Key CBC MAC. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 33–49. Springer (2003)
22) Luby, M., Rackoff, C.: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2), 373386 (1988)
23) McGrew, D.A., Viega, J.: The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 343–355. Springer (2004)
24) Minematsu, K.: Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 275–292. Springer (2014)
25) Namprempre, C., Rogaway, P., Shrimpton, T.: Reconsidering Generic Composition. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 257–274. Springer (2014)
26) NIST Federal Information Processing Standards Publication 198-1. The Keyed-Hash Message Authentication Code (HMAC) (2008)
27) Niwa, Y., Ohashi, K., Minematsu, K., Iwata, T.: GCM Security Bounds Reconsidered. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 385–407. Springer (2015)
28) Rogaway, P., Bellare, M., Black, J.: OCB: A block-cipher mode of operation for efficient authenticated en- cryption. ACM Trans. Inf. Syst. Secur. 6(3), 365–403 (2003)
29) Wegman, M.N., Carter, L.: New Hash Functions and Their Use in Authentication and Set Equality. J. Comput. Syst. Sci. 22(3), 265–279 (1981)