暗号利用モードおよびメッセージ認証コードに関する安全性評価

廣瀬勝一
福井大学　工学研究科

平成23年1月31日

目 次

第1章　まえがき

本稿は以下に掲載されている暗号アルゴリズムの安全性に関する評価結果報告書である．

- NIST SP 800-38A [9]
- NIST SP 800-38B [11]
- NIST SP 800-38C [10]
- NIST SP 800-38D [12]
- ISO/IEC 9797-1 [16]
- NIST FIPS 198-1 [31]

本報告書の構成は以下のとおりである．2章では，評価対象となる暗号アルゴリズムの構成要素であるブロック暗号とハッシュ関数，およびそれらに要求される安全性の定義について記す．2章では，本報告書を通して使用する表記法についても記す．3章では，評価対象となる暗号アルゴリズムである共通鍵暗号化方式，メッセージ認証コード，共通鍵認証付暗号化方式，およびそれらの安全性について記す．4章では，NIST SP 800-38A の5個の守秘用暗号利用モードとその安全性に関する評価結果を述べる．5章では，NIST SP 800-38B の認証用暗号利用モードとその安全性に関する評価結果を述べる．6章では，NIST SP 800-38C の守秘用および認証用暗号利用モードとその安全性に関する評価結果を述べる．7章では，NIST SP 800-38D の守秘用および認証用暗号利用モードとその安全性に関する評価結果を述べる．8章では，ISO/IEC 9797-1 の6個の認証用暗号利用モードとその安全性に関する評価結果を述べる．9章では，NIST FIPS 198-1 のハッシュ関数を用いたメッセージ認証コードとその安全性に関する評価結果を述べる．

第2章　準備

2.1　表記法

本節では本報告書を通して使用する表記法について記す．

$\Sigma = \{0,1\}$ と定義する．Σ^ℓ を長さ $\ell\,(\geq 1)$ のすべての二値系列の集合とみなす．さらに，$(\Sigma^\ell)^* = \bigcup_{i=0}^{\infty}(\Sigma^\ell)^i$, $(\Sigma^\ell)^+ = \bigcup_{i=1}^{\infty}(\Sigma^\ell)^i$, $(\Sigma^\ell)^{\leq m} = \bigcup_{i=0}^{m}(\Sigma^\ell)^i$ と定義する．例えば，$(\Sigma^\ell)^*$ は，空列を含む長さが ℓ の倍数のすべての二値系列の集合を表す．

二値系列 x, y の連接を $x\|y$ と表記する．$\mathsf{lsb}_s(x)$ は x の下位 s ビットを表す．$\mathsf{msb}_s(x)$ は x の上位 s ビットを表す．$\mathsf{len}(x)$ は x のビット長である．また，$x \ll a \stackrel{\text{def}}{=} \mathsf{lsb}_{\mathsf{len}(x)-a}(x)\|0^a$ と定義する．

定義域が $\mathcal{X}$ で値域が $\mathcal{Y}$ のすべての関数の集合を $\mathcal{F}(\mathcal{X},\mathcal{Y})$ と表記する．また，$\mathcal{X}$ 上のすべての置換の集合を $\mathcal{P}(\mathcal{X})$ と表記する．

2.2　構成要素

本報告書の評価対象である暗号アルゴリズムの主要な構成要素は，ブロック暗号とハッシュ関数である．本節では，ブロック暗号とハッシュ関数，および，暗号アルゴリズムの安全性を保証するためにこれらに要求される性質について記す．

2.2.1　ブロック暗号

ブロック暗号は暗号化関数と復号関数からなる．暗号化関数と復号関数はともに鍵付きの置換である．本報告書では，暗号化関数を E, 復号関数を D と表記する．$E : \Sigma^\kappa \times \Sigma^b \to \Sigma^b$, $D : \Sigma^\kappa \times \Sigma^b \to \Sigma^b$ で，Σ^κ は鍵空間である．κ は鍵長，b はブロック長と呼ばれる．任意の $K \in \Sigma^\kappa$, $P \in \Sigma^b$ について，$D(K, E(K, P)) = P$ が成立する．$E(K,\cdot)$, $D(K,\cdot)$ はしばしば，$E_K(\cdot)$, $D_K(\cdot)$ と表記され，本報告書でもそれにしたがう．

2.2.2　ハッシュ関数

ハッシュ関数は，(実用上十分な長さ以下の）任意長の入力系列を固定長の出力系列に変換する関数である．ハッシュ関数の出力系列は，ハッシュ値，ダイジェストなどと呼ばれる．ハッシュ関数は，通常，固定長入出力の関数と，それを用いて任意長の入力を処理して出力を得る方法からなる．この方法は定義域拡大と呼ばれる．

現在広く用いられているハッシュ関数である SHA-1 や SHA-2 (SHA-224/256/384/512) は，圧縮関数と呼ばれる固定長入出力の関数と，Merkle-Damgård 定義域拡大からなる．

圧縮関数を $h : \Sigma^b \times \Sigma^c \to \Sigma^c$ とすると，Merkle-Damgård 定義域拡大によるハッシュ関数 H は以下のとおりである．

1. b の倍数長の入力 M について，$M = M_1 \| M_2 \| \cdots \| M_n$ とする．ここで，$1 \leq i \leq n$ について，$M_i \in \Sigma^b$ である．
2. $s_0 = IV$ とする．IV はあらかじめ定められた初期値である．
3. $1 \leq i \leq n$ について，$s_i = h(s_{i-1}, M_i)$．
4. $s_n = H(M)$ とする．

入力 M の長さが b の倍数でないときは，まず，M に適当な系列を付加して長さを b の倍数とする処理が行われる．この処理はパディングと呼ばれる．H の構成を図 2.1 に示す．

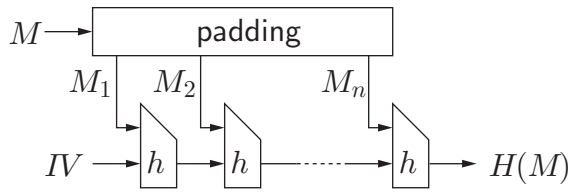


図 2.1: Merkle-Damgård 定義域拡大によるハッシュ関数 H

ハッシュ関数におけるパディング処理では一般に，入力 M の後ろに $\mathsf{len}(M)$ の 2 進数表記を含む系列を付加する．このようなパディングは Merkle-Damgård 強化と呼ばれる．

2.2.3 安全性

ブロック暗号の安全性は，ランダム関数あるいはランダム置換との識別不能性として定式化される．また，ハッシュ関数を用いてメッセージ認証コードを構成する際には，メッセージ認証コードの安全性を保証するために，ハッシュ関数あるいはその圧縮関数をある鍵入力を有する鍵付き関数とみなし，ランダム関数との識別不能性を考える場合がある．

擬似ランダム関数と擬似ランダム置換　$\mathcal{X}$ から $\mathcal{Y}$ への関数族 $f : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ を $\mathcal{X}$ から $\mathcal{Y}$ への鍵付き関数とみなす．ここで $\mathcal{K}$ は鍵空間である．$f(K, \cdot)$ をしばしば f_K と表記する．A を，$\mathcal{X}$ から $\mathcal{Y}$ への関数をオラクルとして 0 または 1 を出力する確率アルゴリズムとする．f に対する A の prf 優位度は

$$\mathrm{Adv}_f^{\mathrm{prf}}(A) = \Pr[A^{f_K} = 1] - \Pr[A^{\rho} = 1]$$

と定義される．ここで，K は $\mathcal{K}$ 上の一様分布に従う確率変数であり，ρ は $\mathcal{F}(\mathcal{X}, \mathcal{Y})$ 上の一様分布に従う確率変数である．計算時間 t 以下で質問回数 q 以下の任意の A について，$\mathrm{Adv}_f^{\mathrm{prf}}(A) \leq \varepsilon$ のとき，f を $(t, q; \varepsilon)$ 擬似ランダム関数 ($(t, q; \varepsilon)$-PRF (pseudorandom function)) と呼ぶ．

$\mathcal{X}$ 上の置換族 $f : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ を $\mathcal{X}$ 上の鍵付き置換とみなす．f に対する A の prp 優位度は

$$\mathrm{Adv}_f^{\mathrm{prp}}(A) = \Pr[A^{f_K} = 1] - \Pr[A^{\rho} = 1]$$

と定義される．ここで，K は $\mathcal{K}$ 上の一様分布に従う確率変数であり，ρ は $\mathcal{P}(\mathcal{X})$ 上の一様分布に従う確率変数である．計算時間 t 以下で質問回数 q 以下の任意の A について，$\mathrm{Adv}_f^{\mathrm{prp}}(A) \leq \varepsilon$ のとき，f を $(t, q; \varepsilon)$ 擬似ランダム置換 ($(t, q; \varepsilon)$-PRP (pseudorandom permutation)) と呼ぶ．

関連鍵攻撃の下での擬似ランダム関数と擬似ランダム置換　$\Phi \subset \mathcal{F}(\mathcal{K}, \mathcal{K})$ とする．A を，関数 $(u, K) \in \mathcal{F}(\mathcal{K} \times \mathcal{X}, \mathcal{Y}) \times \mathcal{K}$ をオラクルとし，0 または 1 を出力する確率アルゴリズムとする．A は $(\phi, x) \in \Phi \times \mathcal{X}$ を質問して $u(\phi(K), x)$ を得ることができる．f に対する A の Φ-rka-prf 優位度は

$$\mathrm{Adv}_{\Phi,f}^{\text{rka-prf}}(A) = \Pr[A^{(f,K)} = 1] - \Pr[A^{(\rho,K)} = 1]$$

と定義される．ここで，K は $\mathcal{K}$ 上の一様分布に従う確率変数であり，ρ は $\mathcal{F}(\mathcal{K} \times \mathcal{X}, \mathcal{Y})$ 上の一様分布に従う確率変数である．計算時間 t 以下で質問回数 q 以下の任意の A について，$\mathrm{Adv}_{\Phi,f}^{\text{rka-prf}}(A) \leq \varepsilon$ のとき，f を $(t, q; \varepsilon)$-Φ-RKA-PRF と呼ぶ．

$\mathcal{P}(\mathcal{K} \times \mathcal{X}, \mathcal{X})$ を $\mathcal{X}$ 上のすべての鍵付き置換の集合とする．$\mathcal{K}$ は鍵空間である．f に対する A の Φ-rka-prp 優位度は

$$\mathrm{Adv}_{\Phi,f}^{\text{rka-prp}}(A) = \left|\Pr[A^{(f,K)} = 1] - \Pr[A^{(\rho,K)} = 1]\right|$$

と定義される．ここで，K は $\mathcal{K}$ 上の一様分布に従う確率変数であり，ρ は $\mathcal{P}(\mathcal{K} \times \mathcal{X}, \mathcal{X})$ 上の一様分布に従う確率変数である．計算時間 t 以下で質問回数 q 以下の任意の A について，$\mathrm{Adv}_{\Phi,f}^{\text{rka-prp}}(A) \leq \varepsilon$ のとき，f を $(t, q; \varepsilon)$-Φ-RKA-PRP と呼ぶ．

第3章　暗号アルゴリズム

3.1　共通鍵暗号化方式

3.1.1　構成

守秘用暗号利用モードは，ブロック暗号を利用して構成される共通鍵暗号化方式である．共通鍵暗号化方式は，鍵生成アルゴリズム $\mathcal{K}$，暗号化アルゴリズム $\mathcal{E}$，復号アルゴリズム $\mathcal{D}$ からなる．

平文空間を $\mathsf{MS} \subseteq \Sigma^*$ とする．暗号化方式では一般に，暗号文の長さから対応する平文の長さが判るので，暗号文の長さから平文に関する長さ以外の有意な情報が得られることを防ぐため，ある長さの系列が MS に属するならば，それと同じ長さの系列はすべて MS に属するものとする．すなわち，$x \in \mathsf{MS}$ ならば $\Sigma^{\mathsf{len}(x)} \subseteq \mathsf{MS}$ とする．さらに，鍵空間を $\mathsf{KS} \subseteq \Sigma^*$ とし，暗号文空間を $\mathsf{CS} = \Sigma^*$ とする．

鍵生成アルゴリズム $\mathcal{K}$ は，$\mathcal{E}, \mathcal{D}$ で用いられる秘密鍵 $K \in \mathsf{KS}$ を生成する確率アルゴリズムである．$\mathcal{K}$ への入力は生成すべき鍵の長さである．与えられた長さが κ であるとき，K は通常，$\Sigma^\kappa \subset \mathsf{KS}$ から一様分布に基づいて無作為に選択される．$\mathcal{E}$ は，与えられた平文 $M \in \mathsf{MS}$ を秘密鍵 K で暗号化して暗号文 $C \in \mathsf{CS}$ を生成するアルゴリズムである．$\mathcal{D}$ は，与えられた暗号文 $C \in \mathsf{CS}$ を秘密鍵 K で復号して平文 M を復元するアルゴリズムである．任意の $K \in \mathsf{KS}$, $M \in \mathsf{MS}$ に対して，$\mathcal{D}_K(\mathcal{E}_K(M)) = M$ の成立することが要求される．なお，$C \in \mathsf{CS}$ について，$K \in \mathsf{KS}$ での復号による対応する平文が存在しないとき，$\mathcal{D}_K(C) = \perp$ とする．

暗号化方式では，暗号文がカウンタ等の状態に依存して決定される場合がある．この状態は暗号化の度毎に更新される．

3.1.2　安全性

選択平文攻撃に対する安全性

Bellare, Desai, Jokipii, Rogaway は，共通鍵暗号化方式に関して，適応的選択平文攻撃に対する四種の安全性を定義し，相互の関係を明らかにしている [4]．本節ではそれらについて記す．

Real-or-Random　この定義は，攻撃者の選択した平文に対応する暗号文と，その平文と同じ長さの無作為に選択された系列の暗号文との識別不能性である．

定義 3.1 (Real-or-Random) A を計算時間 t 以下，質問回数 q 以下の任意の攻撃者とする．また，A の質問の総ビット長を μ 以下とする．暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が

$$\mathrm{Adv}^{\mathrm{rr}}_{ENC}(A) = \Pr[A^{\mathcal{E}_K} = 1] - \Pr[A^{\mathcal{E}'_K} = 1] \leq \varepsilon$$

を満たすとき，ENC は real-or-random の意味で $(t, q, \mu; \varepsilon)$ 安全であると言う．ここで，K は KS 上の一様分布に従う確率変数である．また，$\mathcal{E}'_K$ は，質問 x に対して，x' を $\Sigma^{|x|}$ から一様分布に基づいて選択し，$\mathcal{E}_K(x')$ を返す．

攻撃アルゴリズムが現実的に実行可能であると考えられる任意の t, q, μ に対して，ε が無視できる程度に小さいとき，暗号化方式 ENC は real-or-random の意味で安全であると言われる．一方，攻撃アルゴリズムが現実的に実行可能であると考えられるある t, q, μ に対して，ε が無視できない程度に大きいとき，暗号化方式 ENC は real-or-random の意味で安全でないと言われる．これらの言い回しは，以下の他の意味の安全性に関しても同様に用いられる．

Left-or-Right　この定義では，攻撃者の選択した同じ長さの二つの平文のうち，一方のみが暗号化され，攻撃者に渡される．攻撃者がその暗号文がどちらの平文に対応するか，当てずっぽうと同程度にしか正しく判定できないとき，暗号化方式は安全であると考えられる．

定義 3.2 (Left-or-Right) A を計算時間 t 以下，質問回数 q 以下の任意の攻撃者とする．また，A の質問の総ビット長を μ 以下とする．暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が

$$\mathrm{Adv}^{\mathrm{lr}}_{ENC}(A) = \Pr[A^{\mathcal{E}_K(\mathsf{left}(\cdot,\cdot))} = 1] - \Pr[A^{\mathcal{E}_K(\mathsf{right}(\cdot,\cdot))} = 1] \leq \varepsilon$$

を満たすとき，ENC は left-or-right の意味で $(t, q, \mu; \varepsilon)$ 安全であると言う．ここで，K は KS 上の一様分布に従う確率変数である．また，A の各質問は平文の組 (x_1, x_2) で，$\mathsf{len}(x_1) = \mathsf{len}(x_2)$，$\mathsf{left}(x_1, x_2) = x_1$, $\mathsf{right}(x_1, x_2) = x_2$ である．なお，(x_1, x_2) の長さを $\mathsf{len}(x_1)$ と定める．

Find-then-Guess　この定義は [15, 29] の polynomial security に基づく．この定義では，攻撃者は二段階で動作する．攻撃者を $A = (A_1, A_2)$ とする．第一段階で，攻撃者 A_1 は，等しい長さの二つの平文 x_0, x_1 と保持しておきたい状態の情報 s を出力する．第二段階で，攻撃者 A_2 は，無作為に選択された x_0, x_1 のうちの一方の暗号文 y と s とを入力として受け取り，y がどちらの暗号文であるかを判定する．攻撃者が当てずっぽうと同程度にしか正しく判定できないとき，暗号化方式は安全であると考えられる．

定義 3.3 (Find-then-Guess) $A = (A_1, A_2)$ を計算時間 t 以下，質問回数 q 以下の任意の攻撃者とする．また，A の質問の総ビット長を μ 以下とする．暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が

$$\mathrm{Adv}^{\mathrm{fg}}_{ENC}(A) = 2 \cdot \Pr[(x_0, x_1, s) \leftarrow A_1^{\mathcal{E}_K} : A_2^{\mathcal{E}_K}(\mathcal{E}_K(x_r), s) = r] - 1 \leq \varepsilon$$

を満たすとき，ENC は find-then-guess の意味で $(t, q, \mu; \varepsilon)$ 安全であると言う．ここで，K は KS 上の一様分布に従う確率変数であり，r は Σ 上の一様分布に従う確率変数である．また，$\mathsf{len}(x_0) = \mathsf{len}(x_1)$ である．

Semantic　この定義は [15, 29] の semantic security に基づく．$f : \mathsf{MS} \to \Sigma^*$ とする．任意の m について，MS 上の確率分布の集合 $\mathcal{M} = \{\mathcal{M}_\gamma \,|\, \gamma \in \Sigma^{\leq m}\}$ を考える．これを m 分布と呼ぶ．さらに，各確率分布は妥当，すなわち，任意の $\gamma \in \Sigma^{\leq m}$ について，$\mathcal{M}_\gamma$ の確率非零のすべての系列の長さは等しく，かつ，m 以下であると仮定する．また，$p^*_{f,\mathcal{M}_\gamma} = \max_y\{\Pr[f(X) = y]\}$ と定義する．ここで，X は $\mathcal{M}_\gamma$ に従う確率変数である．

定義 3.4 (Semantic) $f : \mathsf{MS} \to \Sigma^*$ とし，$\mathcal{M} = \{\mathcal{M}_\gamma \,|\, \gamma \in \Sigma^{\leq m}\}$ を MS 上の m 分布とする．A を計算時間 t 以下，質問回数 q 以下の任意の攻撃者とする．また，A の質問の総ビット長を μ 以下とする．暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が

$$\mathrm{Adv}^{\mathrm{s}}_{ENC,f,\mathcal{M}}(A) = \mathbf{E}[\alpha(K, \gamma, s)] \leq \varepsilon$$

を満たすとき，ENC は semantic の意味で $\mathcal{M}$ 上の f に関して $(t, q, \mu; \varepsilon)$ 安全であると言う．ここで，K は KS 上の一様分布に従う確率変数であり，$(\gamma, s) \leftarrow A^{\mathcal{E}_K}(\mathsf{select})$ である．さらに，

$$\alpha(K, \gamma, s) = \Pr[A^{\mathcal{E}_K}(\mathsf{predict}, y, s) = f(x)] - p^*_{f,\mathcal{M}_\gamma}$$

であり，ここで，$x \leftarrow \mathcal{M}_\gamma$, $\mathcal{E}_K(x) = y$ である．

相互の関係　Bellare, Desai, Jokipii, Rogaway [4] は，上記の四種の安全性の相互の関係を詳細に述べているが，ここでは，本報告書に関連して重要と考えられる結果のみを記す．

以下に示す結果より，real-or-random の意味での安全性と left-or-right の意味での安全性は，定数倍の範囲で等価であり，暗号化方式は，これらのいずれかの意味で安全性であれば，他の三つの意味でも安全であることが判る．

定理 3.1 (Real-or-Random ⇒ Left-or-Right) ある正定数 c について，暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が real-or-random の意味で $(t_1, q_1, \mu_1; \varepsilon_1)$ 安全であれば，ENC は left-or-right の意味で $(t_2, q_2, \mu_2; \varepsilon_2)$ 安全である．ここで，$t_2 = t_1 - c\,\mu_2$, $q_2 = q_1$, $\mu_2 = \mu_1$, $\varepsilon_2 = 2\,\varepsilon_1$ である．

定理 3.2 (Left-or-Right ⇒ Real-or-Random) ある正定数 c について，暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が left-or-right の意味で $(t_2, q_2, \mu_2; \varepsilon_2)$ 安全であれば，ENC は real-or-random の意味で $(t_1, q_1, \mu_1; \varepsilon_1)$ 安全である．ここで，$t_1 = t_2 - c\,\mu_1$, $q_1 = q_2$, $\mu_1 = \mu_2$, $\varepsilon_1 = \varepsilon_2$ である．

定理 3.3 (Left-or-Right ⇒ Find-then-Guess) ある正定数 c について，暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が left-or-right の意味で $(t_2, q_2, \mu_2; \varepsilon_2)$ 安全であれば，ENC は find-then-guess の意味で $(t_3, q_3, \mu_3; \varepsilon_3)$ 安全である．ここで，$t_3 = t_2 - c\,\mu_3$, $q_3 = q_2$, $\mu_3 = \mu_2$, $\varepsilon_3 = \varepsilon_2$ である．

定理 3.4 (Real-or-Random ⇒ Semantic) f を時間 $T_f(\cdot)$ で計算可能な関数とし，$\mathcal{M}$ を時間 $T_{\mathcal{M}}(\cdot)$ でサンプル可能な MS 上の妥当な m 分布とする．ある正定数 c について，暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ が real-or-random の意味で $(t_1, q_1, \mu_1; \varepsilon_1)$ 安全であれば，ENC は semantic の意味で $\mathcal{M}$ 上の f に関して $(t_4, q_4, \mu_4; \varepsilon_4)$ 安全である．ここで，$t_4 = t_1 - T_{\mathcal{M}}(m) + T_f(m) - c\mu_4$, $q_4 = q_1 - 1$, $\mu_4 = \mu_1 - m$, $\varepsilon_4 = \varepsilon_1$ である．

選択暗号文攻撃に対する安全性

Katz と Yung は状態を持たない確率的共通鍵暗号化方式の選択平文攻撃および選択暗号文攻撃に対する安全性を定式化し，相互の関連を明らかにしている [24, 25]．本節ではそれについて記す．なお，Katz と Yung は，文献 [4] のような具体的安全性 (concrete security) ではなく，漸近的安全性 (asymptotic security)，すなわち，確率多項式時間の攻撃者に対する安全性として定式化している．この定式化を具体的安全性の定式化に変換することは容易であるが，記述が煩雑になるため，以下でも漸近的安全性のまま記す．

定義 3.5 (識別不能性) $A = (A_1, A_2)$ を暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ に対する攻撃者とする．$X, Y \in \{0, 1, 2\}$ とセキュリティパラメータ k について，A の識別不能性に関する優位度を

$$\mathrm{Adv}^{\text{IND-P}X\text{-CY}}_{ENC}(A, k) = 2 \cdot \Pr[(x_0, x_1, s) \leftarrow A_1^{\mathcal{O}_1, \mathcal{O}'_1}(1^k) : A_2^{\mathcal{O}_2, \mathcal{O}'_2}(1^k, \mathcal{E}_K(x_r), s) = r] - 1$$

と定義する．ここで，

- $X = 0$ のとき，$\mathcal{O}_1 = \mathtt{null}$, $\mathcal{O}_2 = \mathtt{null}$,
- $X = 1$ のとき，$\mathcal{O}_1 = \mathcal{E}_K$, $\mathcal{O}_2 = \mathtt{null}$,
- $X = 2$ のとき，$\mathcal{O}_1 = \mathcal{E}_K$, $\mathcal{O}_2 = \mathcal{E}_K$

であり，

- $Y = 0$ のとき，$\mathcal{O}'_1 = \mathtt{null}$, $\mathcal{O}'_2 = \mathtt{null}$,
- $Y = 1$ のとき，$\mathcal{O}'_1 = \mathcal{D}_K$, $\mathcal{O}'_2 = \mathtt{null}$,
- $Y = 2$ のとき，$\mathcal{O}'_1 = \mathcal{D}_K$, $\mathcal{O}'_2 = \mathcal{D}_K$

である．null はオラクルが存在しないことを表す．K は KS 上の一様分布に従う確率変数であり，r は Σ 上の一様分布に従う確率変数である．また，$\mathsf{len}(x_0) = \mathsf{len}(x_1)$ である．

IND-P2-C0 は前節の Find-then-Guess と同じ定義である．

頑強性 (non-malleabity) の定義では次のような攻撃者を考える．攻撃は，識別不能性の場合と同様に二段階で行われる．第一段階で，攻撃者はメッセージ空間上の確率分布 $\mathcal{M}$ と状態の情報 s を出力する．次に二つの平文 $x, \tilde{x}$ が $\mathcal{M}$ に基づいて独立に選択され，x の暗号文 y が計算される．第二段階で，攻撃者は y と s が与えられ，ある関係 R と暗号文のベクトル $\vec{y}$ を出力する．$\vec{y}$ に対応する平文を $\vec{x}$ とする．任意の確率多項式時間の攻撃者について，$R(x, \vec{x})$ が真である確率と $R(\tilde{x}, \vec{x})$ が真である確率との差が無視できるほど小さい時，暗号化方式は頑強性を満たすという．定義は以下のとおりである．

定義 3.6 (頑強性) $A = (A_1, A_2)$ を暗号化方式 $ENC = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ に対する攻撃者とする．$X, Y \in \{0, 1, 2\}$ とセキュリティパラメータ k について，A の頑強性に関する優位度を

$$\mathrm{Adv}^{\text{NM-P}X\text{-CY}}_{ENC}(A, k) = \mathrm{Expt}^{\text{NM-P}X\text{-CY}}_{ENC}(A, k) - \mathrm{Rand}^{\text{NM-P}X\text{-CY}}_{ENC}(A, k).$$

と定義する．ここで，

$$\mathrm{Expt}^{\text{NM-P}X\text{-CY}}_{ENC}(A,k) =$$
$$\Pr\Big[K \leftarrow \mathsf{KS}; (\mathcal{M},s) \leftarrow A_1^{\mathcal{O}_1,\mathcal{O}'_1}(1^k); x \leftarrow \mathcal{M}; y \leftarrow \mathcal{E}_K(x);$$
$$(R,\vec{y}) \leftarrow A_2^{\mathcal{O}_2,\mathcal{O}'_2}(1^k,y,s); \vec{x} = \mathcal{D}_K(\vec{y}) : y \neq \perp \wedge y \notin \vec{y} \wedge \perp \notin \vec{x} \wedge R(x,\vec{x})\Big]$$

$$\mathrm{Rand}^{\text{NM-P}X\text{-CY}}_{ENC}(A,k) =$$
$$\Pr\Big[K \leftarrow \mathsf{KS}; (\mathcal{M},s) \leftarrow A_1^{\mathcal{O}_1,\mathcal{O}'_1}(1^k); x,\tilde{x} \leftarrow \mathcal{M}; y \leftarrow \mathcal{E}_K(x);$$
$$(R,\vec{y}) \leftarrow A_2^{\mathcal{O}_2,\mathcal{O}'_2}(1^k,y,s); \vec{x} = \mathcal{D}_K(\vec{y}) : y \neq \perp \wedge y \notin \vec{y} \wedge \perp \notin \vec{x} \wedge R(\tilde{x},\vec{x})\Big]$$

である．X, Y の値に対応するオラクル $\mathcal{O}_1$, $\mathcal{O}'_1$, $\mathcal{O}_2$, $\mathcal{O}'_2$ は，定義 3.5 と同じである．

定義 3.5 と定義 3.6 より 18 個の安全性の概念が得られるが，それら相互の関係は図 3.1 のとおりである．

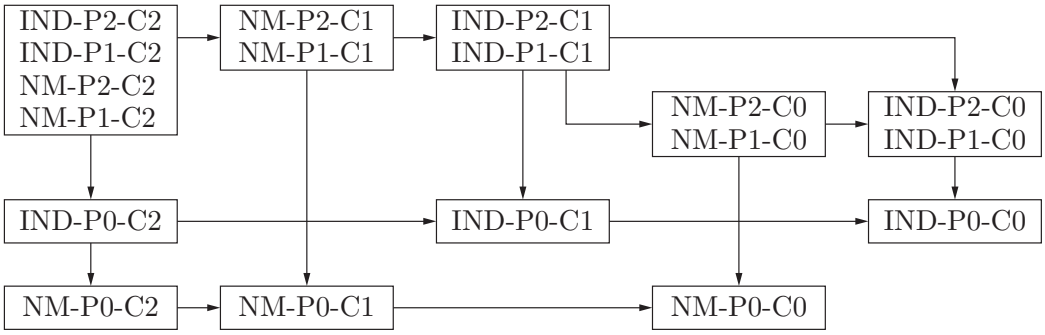


図 3.1: 共通鍵暗号化方式の安全性の概念の関係．同じ枠内の安全性の概念は等価である．また，各矢印について，その始点の安全性の概念はその終点の安全性の概念より真に強い概念である．

3.2 メッセージ認証コード

3.2.1 構成

メッセージ認証コード (Message Authentication Code, MAC) は，メッセージの改ざんを防止するための暗号アルゴリズムであり，鍵生成アルゴリズム $\mathcal{K}$，認証子生成アルゴリズム $\mathcal{G}$，認証子検証アルゴリズム $\mathcal{V}$ からなる．

$\mathcal{K}$ は，$\mathcal{G}, \mathcal{V}$ で用いられる秘密鍵 K を生成する確率アルゴリズムである．なお，K は通常，鍵空間 KS から一様分布に基づいて無作為に選択される．$\mathcal{G}$ は，秘密鍵 K と与えられたメッセージ M から，そのメッセージの認証子 T を生成するアルゴリズムである．$\mathcal{V}$ は，秘密鍵 K と与えられたメッセージと認証子の組 (M,T) について，T が K による M に対する正しい認証子であるかどうかを検証するアルゴリズムである．

3.2.2 安全性

メッセージ認証コードの安全性は，適応的選択文書攻撃に対する偽造不能性として定義される [5, 6].

メッセージ認証コードに対する攻撃者 A は，$\mathcal{G}_K$ をオラクルとし，メッセージを質問してそれに対する認証子を得ることができる．A がオラクルに質問していないメッセージに対して正しい認証子を作成することに成功したとき，A は偽造に成功したという．

定義 3.7 A を計算時間 t 以下，質問回数 q 以下の任意の偽造攻撃者とする．また，A の質問の総ビット長を μ 以下とする．メッセージ認証コード $MAC = (\mathcal{K}, \mathcal{G}, \mathcal{V})$ が

$$\mathrm{Adv}^{\mathrm{mac}}_{MAC}(A) = \Pr[A^{\mathcal{G}_K} \text{ が偽造に成功}] \leq \varepsilon$$

を満たすとき，MAC は存在偽造に関して $(t, q, \mu; \varepsilon)$ 安全であると言う．ここで，K は KS 上の一様分布に従う確率変数である．

上記の定義では，質問の総ビット長をパラメータとしているが，定義によっては，最長の質問のメッセージブロック数を用いる場合などもある．

メッセージ認証コードの安全性は，しばしば，2.2.3 節に記したランダム関数との識別不能性（擬似ランダム関数）の観点からも評価される．この場合も，パラメータとして，計算時間と質問回数の他に，質問の総長あるいは最長の質問のブロック数などが付加される．

文献 [6] の命題 2.7 より，メッセージ認証コードの偽造不能性と識別不能性に関して，以下の関係が成立することが判る．

定理 3.5 メッセージ認証コード $MAC = (\mathcal{K}, \mathcal{G}, \mathcal{V})$ について，$\mathcal{G}$ の出力長を τ とする．A を MAC に対する偽造攻撃者とする．A の計算時間を t 以下, 質問回数を q 以下，質問の総長を μ 以下とする．このとき，

$$\mathrm{Adv}^{\mathrm{mac}}_{MAC}(A) \leq \mathrm{Adv}^{\mathrm{prf}}_{\mathcal{G}}(A') + \frac{1}{2^{\tau}}$$

を満たす $\mathcal{G}$ に対する識別攻撃者 A' が存在する．ここで，A' の計算時間は $t + O(\mu + q\tau + \ell)$ 以下，質問回数は $q + 1$ 以下，質問の総長は $\mu + \ell$ 以下である．なお，ℓ は A の出力する偽造のメッセージ長である．

3.3 認証付暗号化方式

本報告書での評価対象である認証付暗号化方式 CCM と GCM はともに，関連データ付き認証付暗号化方式 (Authenticated Encryption with Associated Data, AEAD) と呼ばれる方式である．AEAD の定義とその安全性の定義は Rogaway [34] により与えられている．本節ではそれについて記す．

3.3.1 構成

AEAD は，鍵生成アルゴリズム $\mathcal{K}$, 暗号化アルゴリズム $\mathcal{E}$，復号アルゴリズム $\mathcal{D}$ の三つ組 $AE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ と定義される．さらに，AE は，鍵の集合 KS，nonce の集合 NS，ヘッダの集合 $\mathsf{HS} \subseteq \Sigma^*$，平文の集合 $\mathsf{MS} \subseteq \Sigma^*$，暗号文の集合 $\mathsf{CS} \subseteq \Sigma^*$ を伴う．MS については，$M \in \mathsf{MS}$ ならば $\Sigma^{\mathsf{len}(M)} \subseteq \mathsf{MS}$ とする．

$\mathcal{E}$ は，入力 $K \in \mathsf{KS}$, $N \in \mathsf{NS}$, $H \in \mathsf{HS}$, $M \in \mathsf{MS}$ に対して，$\mathcal{E}_K(N, H, M) = C \in \mathsf{CS}$ を出力する．$\mathcal{D}$ は，入力 $K \in \mathsf{KS}$, $N \in \mathsf{NS}$, $H \in \mathsf{HS}$, $C \in \mathsf{MS}$ に対して，$\mathcal{D}_K(N, H, C) = M \in \mathsf{MS}$ あるいは $\perp$ を出力する．$\perp$ は鍵 K に関して，N, H, C に対応する平文が存在しないことを意味する．

3.3.2 安全性

AEAD の安全性は，守秘性と偽造不能性に関して定義される．なお，攻撃者はオラクルに対して同じ nonce を用いた質問を複数回行わないと仮定される．このような制約を課せられた攻撃者は nonce-respecting と呼ばれる．

定義 3.8 (守秘性) $\$(\cdot,\cdot,\cdot)$ を入力 N, H, M に対して，$\Sigma^{\mathsf{len}(\mathcal{E}_K(N,H,M))}$ に属する系列を無作為に選択して返すオラクルとする．$AE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ に対する識別攻撃者 A の priv 優位度は

$$\mathrm{Adv}^{\mathrm{priv}}_{AE}(A) = \Pr[A^{\mathcal{E}_K} = 1] - \Pr[A^{\$} = 1]$$

と定義される．K は KS 上の一様分布に基づく確率変数である．

上記のような定義は IND$-CPA（選択平文攻撃の下での識別不能性）と呼ばれる．

定義 3.9 (偽造不能性) $AE = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ について，A を $\mathcal{E}_K$ をオラクルとする偽造攻撃者とする．A が以下の条件を満たす (N, H, C) を出力したとき，A は偽造に成功したと言う．

- $\mathcal{D}_K(N, H, C) \neq \perp$
- A は $\mathcal{E}_K(N, H, M) = C$ なる N, H, M をオラクル $\mathcal{E}_K$ に質問していない．

AE に対する偽造攻撃者 A の auth 優位度は

$$\mathrm{Adv}^{\mathrm{auth}}_{AE}(A) = \Pr[A^{\mathcal{E}_K} \text{ が偽造に成功}]$$

と定義される．

第4章　NIST SP 800-38Aの暗号利用モード

本章では，NIST SP 800-38A [9] で規定されている以下の守秘用暗号利用モードについて，それぞれの仕様と安全性評価の結果を報告する．

1. Electronic Codebook Mode (ECB モード)
2. Cipher Block Chaining Mode (CBC モード)
3. Cipher Feedback Mode (CFB モード)
4. Output Feedback Mode (OFB モード)
5. Counter Mode (CTR モード)

ECB モードと CBC モードでは，平文の長さは，使用されるブロック暗号のブロック長 b の倍数でなければならず，ある正整数 n について nb である．このとき，平文は n 個の b ビットの平文ブロック $P_1, P_2, \ldots, P_n$ からなる．

CFB モードでは，平文の長さはパラメータ $s\,(\leq b)$ の倍数でなければならず，ある正整数 n について ns である．このとき，平文は n 個の s ビットの平文ブロック $P_1^{\#}, P_2^{\#}, \ldots, P_n^{\#}$ からなる．

OFB モードと CTR モードでは，平文の長さは任意であり，ある正整数 n と b 以下のある正整数 u について，$(n-1)b+u$ である．このとき，平文は $n-1$ 個の b ビットの平文ブロック $P_1, P_2, \ldots, P_{n-1}$ と u ビットの平文ブロック P_n^* からなる．

すべてのモードで，各平文ブロックは同じ長さの対応する暗号文ブロックに変換される．P_i, $P_i^{\#}$, P_n^* に対応する暗号文ブロックをそれぞれ，C_i, $C_i^{\#}$, C_n^* と表記する．

4.1　ECB モード

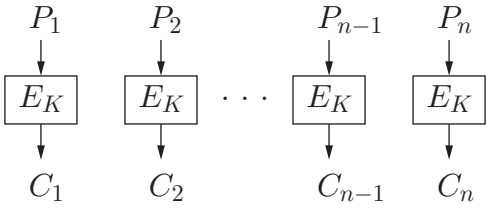
4.1.1　仕様

ECB モードの暗号化と復号は次のように定義されている．

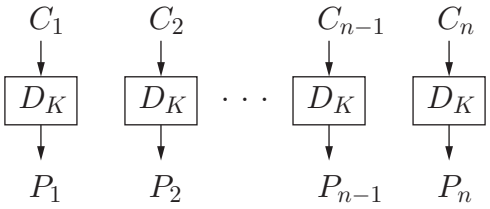
ECB 暗号化　$i = 1, \ldots, n$ について，$C_i = E_K(P_i)$.

ECB 復号　$i = 1, \ldots, n$ について，$P_i = D_K(C_i)$.

ECB モードの暗号化と復号を図 4.1 に示す．



(a) 暗号化



(b) 復号

図 4.1: ECB モード

4.1.2 安全性

識別攻撃

ECB モードは，選択平文攻撃に対して安全な守秘用暗号利用モードではない．例えば，left-or-right の意味での安全性に関して，以下のような攻撃者 A を考える．

1. $P_{\mathrm{l}1} = P_{\mathrm{l}2}$, $P_{\mathrm{r}1} \neq P_{\mathrm{r}2}$ を満たす $P_{\mathrm{l}1}, P_{\mathrm{l}2}, P_{\mathrm{r}1}, P_{\mathrm{r}2} \in \Sigma^b$ を任意に定め，$(P_{\mathrm{l}1} \| P_{\mathrm{l}2}, P_{\mathrm{r}1} \| P_{\mathrm{r}2})$ をオラクルに質問する．

2. オラクルの応答 $C_1 \| C_2$ について，$C_1 = C_2$ ならば 1 を出力し，$C_1 \neq C_2$ ならば 0 を出力する．

このとき，

$$\mathrm{Adv}^{\mathrm{lr}}_{\mathrm{ECB}}(A) = \Pr[A^{\mathcal{E}_K(\mathsf{left}(\cdot,\cdot))} = 1] - \Pr[A^{\mathcal{E}_K(\mathsf{right}(\cdot,\cdot))} = 1] = 1$$

が成立する．

4.2 CBC モード

4.2.1 仕様

CBC モードの暗号化と復号は次のように定義されている．

CBC 暗号化

$$C_i = \begin{cases} E_K(P_1 \oplus IV) & (i = 1) \\ E_K(P_i \oplus C_{i-1}) & (i = 2, \ldots, n). \end{cases}$$

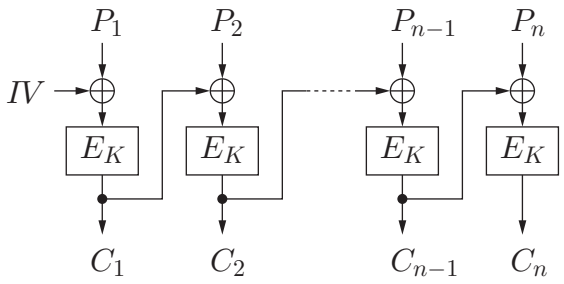
CBC 復号

$$P_i = \begin{cases} E_K(C_1) \oplus IV & (i = 1) \\ E_K(C_i) \oplus C_{i-1} & (i = 2, \ldots, n). \end{cases}$$

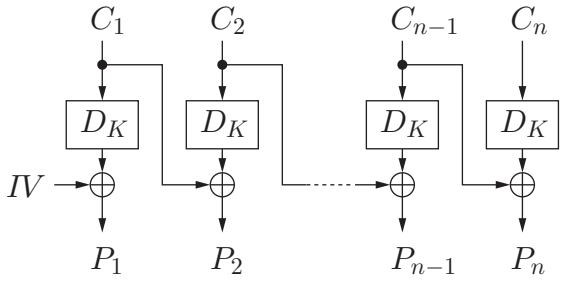
IV は初期ベクトルと呼ばれる．CBC モードの暗号化と復号を図 4.2 に示す．

IV は秘密である必要はないが，予測不能でなければならない．予測不能性を満たす IV の生成法として，NIST SP 800-38A では，以下の二つの方法が推奨されている．

1. nonce を E_K で暗号化する．
2. FIPS の乱数生成器を用いる．



(a) 暗号化



(b) 復号

図 4.2: CBC モード

4.2.2 安全性

証明可能安全性

CBC モードの証明可能安全性に関しては，CBC 暗号化の実行ごとに初期ベクトル IV が無作為に選択される場合について，Bellare, Desai, Jokipii, Rogaway により論じられている [4].

文献 [4] では，定理 17 で，CBC モードのブロック暗号を擬似ランダム関数族に置き換えた場合に関して，left-or-right の意味での安全性が示されている．なお，[4] の命題 9 と補題 16 とを用いると，以下に示す定理 17 と同様の結果を導くことができる．

補題 4.1 (命題 9 [4]) F が入力長・出力長共に b の $(t, q; \varepsilon)$-PRP ならば，F は $(t, q; \varepsilon')$-PRF である．ここで，$\varepsilon' = \varepsilon - q^2/2^{b+1}$ である．

補題 4.2 (補題 16 [4]) A を CBC のブロック暗号をランダム関数で置き換えた暗号化方式（CBC-RF と表記する）に対する攻撃者とする．A の質問回数を q 以下，質問の総長を μ ビット以下とする．このとき，

$$\mathrm{Adv}^{\mathrm{lr}}_{\text{CBC-RF}}(A) \leq \left(\frac{\mu^2}{b^2} - \frac{\mu}{b}\right)\frac{1}{2^b}$$

である．

定理 4.3 E を $(t', q'; \varepsilon')$-PRP と仮定する．このとき，CBC モードは left-or-right の意味で $(t, q, \mu; \varepsilon)$ 安全である．ここで，$\mu = q'b$, $t = t' - O(\mu)$,

$$\varepsilon = 2\varepsilon' + \left(\frac{2\mu^2}{b^2} - \frac{\mu}{b}\right)\frac{1}{2^b}$$

であり，また，$q \leq \mu/b$ である．

nonce を暗号化して IV を生成する方式に対する識別攻撃

前述のとおり，NIST SP 800-38A では，CBC モードに関して，nonce を平文を暗号化する鍵と同じ鍵で暗号化して IV を生成する方法が推奨されている．しかし，この方法に対しては，Rogaway [35] により以下の識別攻撃が与えられている．この攻撃では攻撃者は nonce を選択できると仮定している．また，Real-or-Random の意味での安全性を考える．

1. 攻撃者 A は，$(N^{(1)}, P_1^{(1)} \| P_2^{(1)}) = (0^b, 0^b \| 0^b)$ を質問して，暗号文 $C_1^{(1)} \| C_2^{(1)}$ を得る．
2. A は，$(N^{(2)}, P_1^{(2)}) = (C_1^{(1)}, C_2^{(1)} \oplus C_1^{(1)})$ を質問して，暗号文 $C_1^{(2)}$ を得る．
3. A は，$C_1^{(2)} = C_2^{(1)}$ のとき 1 を出力する．それ以外のとき，0 を出力する．

この攻撃の質問に関する CBC の計算は図 4.3 のとおりである．この攻撃について

$$\mathrm{Adv}^{\mathrm{rr}}_{\mathrm{CBC}}(A) = 1 - 1/2^b$$

である．なお，文献 [35] では，nonce が平文を暗号化する鍵と異なる鍵で暗号化される場合は安全であることが示されている．

暗号文がブロックごとに得られる場合の識別攻撃

適応的選択平文攻撃では，通常，平文 $P_1 \| P_2 \| \cdots \| P_n$ 全体が同時にオラクルに与えられ，それに対して，暗号文 $C_1 \| C_2 \| \cdots \| C_n$ が得られるような状況を仮定する．それに対して，攻撃者が，平文をブロックごとにオラクルに与え，C_i を得た後に P_{i+1} を選択して質問できると仮定すると，任意の v について，$P_{i+1} = C_i \oplus v$ とすることにより，v を E_K

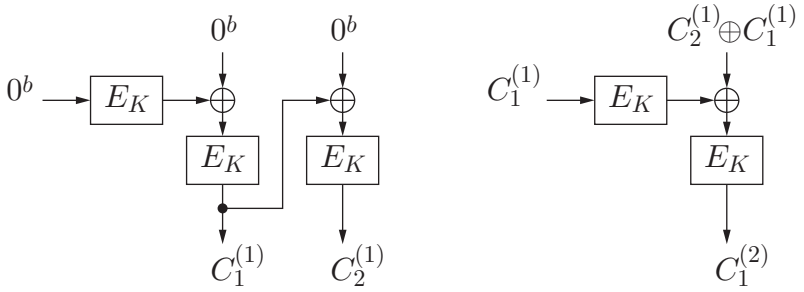


図 4.3: 識別攻撃の質問に対する CBC の計算

への入力とすることができる．これは，攻撃者が初期ベクトル IV を予想できるばかりでなく，自由に選択できることと同等であり，これを利用することにより，自明な識別攻撃が可能となる [22].

上記の攻撃への対策として，Delayed CBC と呼ばれる方法が知られている．この方法では，暗号化オラクルは，P_{i+1} を受け取った後に，C_i を返す．また，最後の暗号文ブロックは，次の平文ブロックが存在しないことを知った後に返す．Delayed CBC の証明可能安全性は Fouque, Martinet, Poupard [13] により示されている．

選択暗号文攻撃に対する安全性

ここでは，CBC モードが，IND-P2-C2 を満たさないこと，すなわち，適応的選択暗号文攻撃に対して識別不能性を満たさないことを示す．攻撃アルゴリズムは以下のとおりである．

1. 攻撃者は，第一段階で，2 ブロックからなる二つの平文 $P^{(0)} = P_1^{(0)} \| P_2^{(0)}$, $P^{(1)} = P_1^{(1)} \| P_2^{(1)}$ を出力する．ただし，$P_1^{(0)} \neq P_1^{(1)}$ とする．

2. 第二段階で，入力された暗号文 $C = C_1 \| C_2$ と IV について，C_2 と異なる C_2' を適当に選び，$C' = C_1 \| C_2'$ と IV を復号オラクルに質問して，対応する平文 $P' = P_1' \| P_2'$ を得る．$P_1' = P_1^{(r)}$ を満たす $r \in \Sigma$ を出力する．

この攻撃者の優位度は 1 である．

4.3 CFB モード

4.3.1 仕様

CFB モードは，正整数のパラメータ $s\,(\leq b)$ を有し，各平文ブロックと暗号文ブロックの長さは s ビットである．CFB モードの暗号化と復号は次のように定義されている．

CFB 暗号化 $i = 1, \ldots, n$ について

$$C_i^{\#} = P_i^{\#} \oplus \mathsf{msb}_s(E_K(I_i)).$$

ここで，

$$I_i = \begin{cases} IV & (i = 1) \\ \mathsf{lsb}_{b-s}(I_{i-1}) \| C_{i-1}^{\#} & (i = 2, \ldots, n) \end{cases}$$

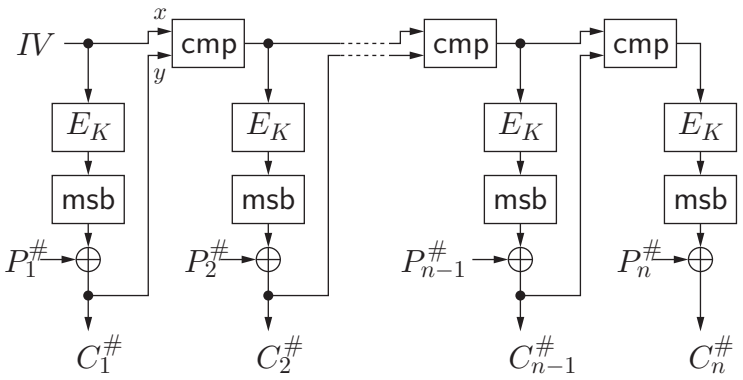
である．

CFB 復号 $i = 1, \ldots, n$ について

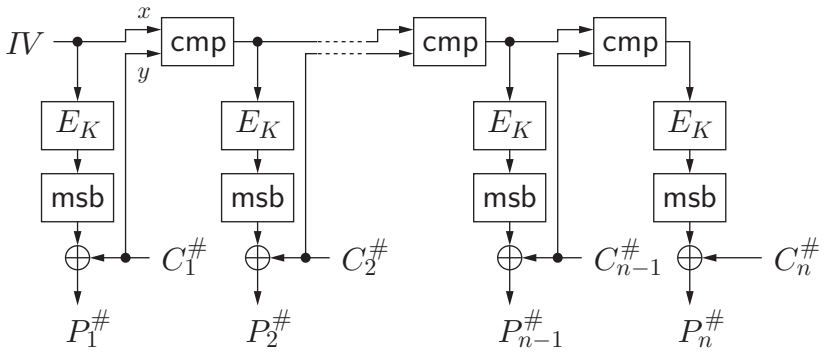
$$P_i^{\#} = C_i^{\#} \oplus \mathsf{msb}_s(E_K(I_i)).$$

IV は初期ベクトルである．CFB モードの暗号化と復号を図 4.4 に示す．

CBC モードと同様に，このモードでも IV は秘密である必要はないが，予測不能でなければならない．予測不能性を満たす IV の生成法として，CBC モードの場合と同じ二つの方法が推奨されている．



(a) 暗号化



(b) 復号

図 4.4: CFB モード．msb は msb_s を表し，$\mathsf{cmp}(x, y)$ は $\mathsf{lsb}_{b-s}(x) \| y$ を表す．

4.3.2 安全性

証明可能安全性

CFB モードの証明可能安全性に関しては，CFB 暗号化を実行するごとに初期ベクトル IV が無作為に選択される場合について，Alkassar, Geraldy, Pfitzmann, Sadeghi により

論じられている [1].

[1] では，定理 1 で，CFB モードのブロック暗号を擬似ランダム関数族に置き換えた場合に関して，left-or-right の意味での安全性が示されている．なお，[4] の命題 9 と [1] の補題 1 とを用いると，以下に示す定理 1 と同様の結果を導くことができる．

補題 4.4 (補題 1 [1]) A を CFB のブロック暗号をランダム関数で置き換えた暗号化方式（CFB-RF と表記する）に対する攻撃者とする．A の質問回数を q 以下，質問の総ビット長を bq 以下とする．このとき，

$$\mathrm{Adv}^{\mathrm{lr}}_{\text{CFB-RF}}(A) \leq q^2/2^{b+1}$$

である．

定理 4.5 E を $(t', q'; \varepsilon')$-PRP と仮定する．このとき，CFB モードは left-or-right の意味で $(t, q, \mu; \varepsilon)$ 安全である．ここで，$q = q'$, $\mu = q's$, $t = t' - O(q's)$,

$$\varepsilon = 2\varepsilon' + \frac{3q^2}{2^{b+1}}$$

である．

選択暗号文攻撃に対する安全性

CFB モードは IND-P2-C2 を満たさない．攻撃アルゴリズムは，CBC モードに対する適応的選択暗号文攻撃と同様であるので省略する．

4.4 OFB モード

4.4.1 仕様

OFB モードの暗号化と復号は次のように定義されている．

OFB 暗号化

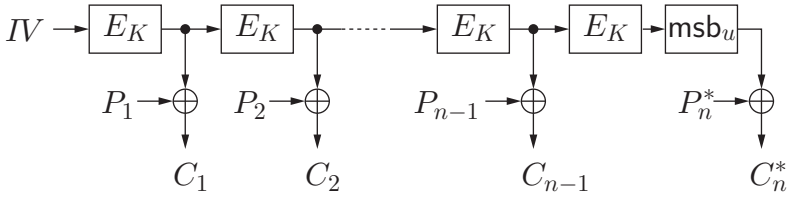
$$C_i = P_i \oplus (\overbrace{E_K \circ \cdots \circ E_K}^{i})(IV) \qquad (i = 1, \ldots, n-1)$$
$$C_n^* = P_n^* \oplus \mathsf{msb}_u((\overbrace{E_K \circ \cdots \circ E_K}^{n})(IV)).$$

OFB 復号

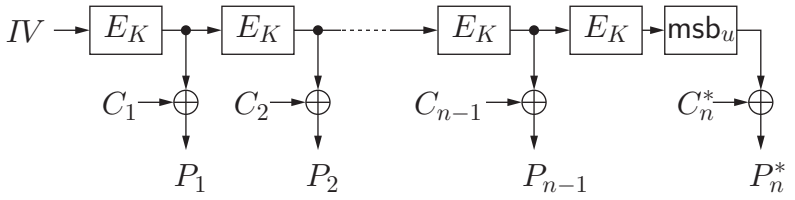
$$P_i = C_i \oplus (\overbrace{E_K \circ \cdots \circ E_K}^{i})(IV) \qquad (i = 1, \ldots, n-1)$$
$$P_n^* = C_n^* \oplus \mathsf{msb}_u((\overbrace{E_K \circ \cdots \circ E_K}^{n})(IV)).$$

IV は初期ベクトルである．OFB モードの暗号化と復号を図 4.5 に示す．

OFB モードでは，IV は予測可能であっても良い．しかし，nonce であることが要求される．すなわち，同じ秘密鍵でモードを実行するごとに異なる値でなければならず，このモードは状態を有する暗号化方式である．NIST SP 800-38A では，カウンタやメッセージ番号を IV として用いることが推奨されている．



(a) 暗号化



(b) 復号

図 4.5: OFB モード

4.4.2 安全性

証明可能安全性

OFB モードの証明可能安全性に関しては，他のモードと同様に議論できる．以下では，OFB 暗号化を実行するごとに初期ベクトル IV が無作為に選択される場合について考える．

補題 4.6 A を OFB のブロック暗号をランダム関数で置き換えた暗号化方式（OFB-RF と表記する）に対する攻撃者とする．A の質問回数を q 以下，質問の総ビット長を μ 以下とする．このとき，

$$\mathrm{Adv}^{\mathrm{lr}}_{\text{OFB-RF}}(A) \leq (\mu/b)^2/2^{b+1}$$

である．

[4] の命題 9 と上の補題とを用いると，次の結果を導くことができる．

定理 4.7 E を $(t', q'; \varepsilon')$-PRP と仮定する．このとき，CFB モードは left-or-right の意味で $(t, q, \mu; \varepsilon)$ 安全である．ここで，$\mu = q'b$, $t = t' - O(\mu)$,

$$\varepsilon = 2\varepsilon' + \frac{3(\mu/b)^2}{2^{b+1}}$$

であり，また，$q \leq \mu/b$ である．

選択暗号文攻撃に対する安全性

OFB モードは IND-P2-C2 を満たさない．攻撃アルゴリズムは，CBC モードに対する適応的選択暗号文攻撃と同様であるので省略する．

4.5 CTR モード

4.5.1 仕様

CTR モードの暗号化と復号は次のように定義されている．なお，以下で，$T_1, \ldots, T_n$ はカウンタの値を表す．

CTR 暗号化

$$
\begin{aligned}
C_i &= P_i \oplus E_K(T_i) \qquad (i = 1, \ldots, n-1) \\
C_n^* &= P_n^* \oplus \mathsf{msb}_u(E_K(T_n))
\end{aligned}
$$

CTR 復号

$$
\begin{aligned}
P_i &= C_i \oplus E_K(T_i) \qquad (i = 1, \ldots, n-1) \\
P_n^* &= C_n^* \oplus \mathsf{msb}_u(E_K(T_n))
\end{aligned}
$$

CTR モードの暗号化と復号を図 4.6 に示す．

なお，この仕様では，同じ秘密鍵で使用されるすべてのカウンタの値が互いに異なることを要求している．これを実現するためには，暗号化の処理において，カウンタに関する情報を状態として保持しなければならない．

4.5.2 安全性

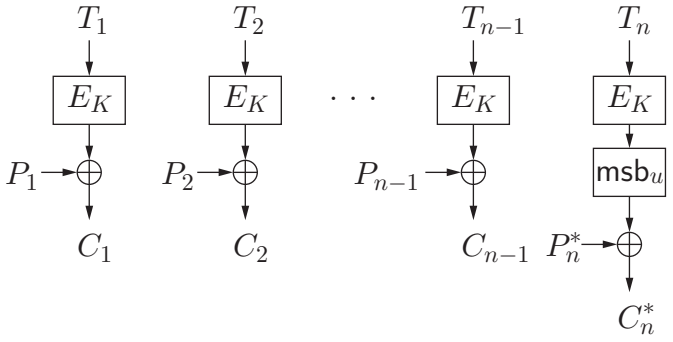
証明可能安全性

CTR モードの証明可能安全性に関しては，以下の二つの場合について，Bellare, Desai, Jokipii, Rogaway により論じられている [4]．

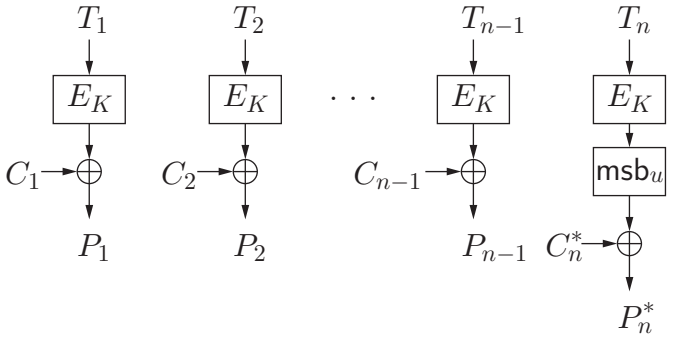
1. 同じ秘密鍵で利用されるカウンタの値がすべて異なる場合．
2. $T_{i+1} = T_i + 1$ であり，CTR 暗号化を実行するごとに T_1 が無作為に選択される場合．

NIST SP 800-38A の CTR モードは 1 番目の場合に相当する．

文献 [4] では，定理 14 で，CTR モードのブロック暗号を擬似ランダム関数族に置き換え，カウンタの値がすべて異なる場合について，left-or-right の意味での安全性が示されている．なお，[4] の命題 9 と補題 13 とを用いると，以下に示す定理 14 と同様の結果を導くことができる．



(a) 暗号化



(b) 復号

図 4.6: CTR モード

補題 4.8 (補題 13 [4]) A を CTR のブロック暗号をランダム関数で置き換えた暗号化方式（CTR-RF と表記する）に対する攻撃者とする．A の質問回数を q 以下，質問の総ビット長を $\mu\,(\leq b2^b)$ 以下とする．このとき，

$$\mathrm{Adv}^{\mathrm{lr}}_{\text{CTR-RF}}(A) = 0$$

である．

定理 4.9 E を $(t', q'; \varepsilon')$-PRP と仮定する．このとき，CTR モードは left-or-right の意味で $(t, q, \mu; \varepsilon)$ 安全である．ここで，$\mu = \min(q'b, b\,2^b)$, $t = t' - O(\mu)$,

$$\varepsilon = 2\varepsilon' + \frac{(\mu/b)^2}{2^b}$$

であり，また，$q \leq \mu/b$ である．

選択暗号文攻撃に対する安全性

CTR モードは IND-P2-C2 を満たさない．攻撃アルゴリズムは，CBC モードに対する適応的選択暗号文攻撃と同様であるので省略する．

4.6 まとめ

NIST SP 800-38A の暗号利用モードについては，ECB モードを除くすべてのモードが，適応的選択平文攻撃に対する証明可能安全性を有しており，AES などの脆弱性の指摘されていないブロック暗号を用いた場合，ブロック長を b とするとき，攻撃に要するブロック暗号の呼出し回数は $\Theta(2^{b/2})$ であると考えられる．この結果より，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては，ECB を除くすべてのモードは，適応的選択平文攻撃に対して安全なモードであると言える．

一方，実用に関しては，以下の点に関する注意が必要である．

- どのモードに対しても容易な適応的選択暗号文攻撃が存在する．
- CBC モードに関しては，以下の場合に対して適応的選択平文攻撃が存在する．
  - 平文ブロックごとに暗号文を得られるような場合
  - nonce を平文と同じ鍵で暗号化して初期ベクトル IV を生成する場合

第5章　NIST SP 800-38BのCMAC

本章では，NIST SP 800-38B [11] で規定されている認証用暗号利用モード CMAC (Cipher-based MAC) の仕様と安全性評価の結果を報告する．CMAC は（出力の切詰めを除いて）岩田と黒澤 [17] により提案された OMAC1 と等価である．

5.1　仕様

サブ鍵生成

1. $L = E_K(0^b)$
2. $K_1 = \begin{cases} L \ll 1 & (\mathsf{msb}_1(L) = 0) \\ (L \ll 1) \oplus R_b & (\mathsf{msb}_1(L) = 1) \end{cases}$
3. $K_2 = \begin{cases} K_1 \ll 1 & (\mathsf{msb}_1(K_1) = 0) \\ (K_1 \ll 1) \oplus R_b & (\mathsf{msb}_1(K_1) = 1) \end{cases}$

なお，R_b は定数であり，$R_{128} = 0^{120}10000111$, $R_{64} = 0^{59}11011$ である．上記の 2, 3 の演算は，$b = 128$ のとき，$\mathrm{GF}(2^{128})$ における $\mathsf{u}^{128} + \mathsf{u}^7 + \mathsf{u}^2 + \mathsf{u} + 1$ を法とする u の乗算，$b = 64$ のとき，$\mathrm{GF}(2^{64})$ における $\mathsf{u}^{64} + \mathsf{u}^4 + \mathsf{u}^3 + \mathsf{u} + 1$ を法とする u の乗算である．これらの多項式は，項数最小の既約多項式のうち，辞書式順序で先頭の多項式である．

MAC生成　MAC 生成アルゴリズム $\mathsf{CMAC}_K(M, \tau)$ は以下のとおりである．M は入力メッセージであり，τ は出力される認証子の長さである．なお，$M = M_1 \| M_2 \| \cdots \| M_{n-1} \| M_n^*$ とし，$1 \le i \le n-1$ について，$\mathsf{len}(M_i) = b$，$0 \le \mathsf{len}(M_n^*) \le b$ とする．ここで，

$$n = \begin{cases} 1 & (\mathsf{len}(M) = 0) \\ \lceil \mathsf{len}(M)/b \rceil & (\mathsf{len}(M) \neq 0) \end{cases}$$

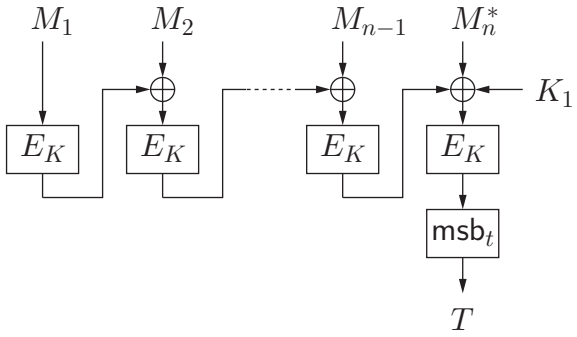
である．したがって，$0 \le \mathsf{len}(M) \le b$ のとき，$M = M_1^*$ である．

1. サブ鍵生成アルゴリズムにより，K から K_1, K_2 を計算する．
2. $M_n = \begin{cases} M_n^* \oplus K_1 & (\mathsf{len}(M_n^*) = b) \\ (M_n^* \| 10^{nb - \mathsf{len}(M) - 1}) \oplus K_2 & (\mathsf{len}(M_n^*) < b) \end{cases}$
3. $C_0 = 0^b$

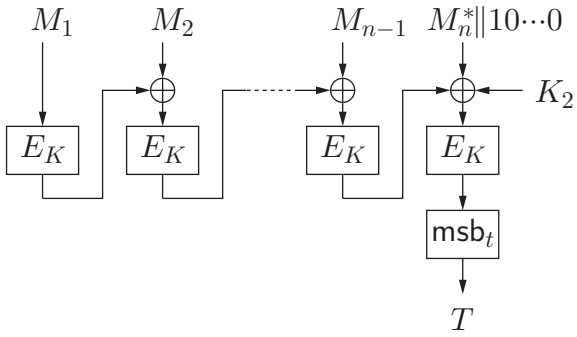
4. $1 \leq i \leq n$ について，$C_i = E_K(C_{i-1} \oplus M_i)$.

5. $T = \mathsf{msb}_\tau(C_n)$ を出力する.

CMAC の MAC 生成を図 5.1 に示す.



(a) $\mathsf{len}(M_n^*) = b$ のとき



(b) $\mathsf{len}(M_n^*) < b$ のとき

図 5.1: CMAC の MAC 生成

MAC 検証　メッセージと認証子の組 (M, T') について，$T' = \mathsf{CMAC}_K(M, \tau)$ であれば `VALID` を，そうでなければ `INVALID` を返す.

5.2　安全性

5.2.1　証明可能安全性

CMAC と等価な OMAC1 の証明可能安全性に関しては，[17, 18] で議論されている．[18] の結果より，以下の定理が成り立つことが判る.

定理 5.1 A を CMAC に対する偽造攻撃者とする．A の計算時間を t 以下，質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，E に対するある prp 攻撃者 A_1 が存在して

$$\mathrm{Adv}^{\mathrm{mac}}_{\mathsf{CMAC}}(A) \leq \mathrm{Adv}^{\mathrm{prp}}_{E}(A_1) + \frac{4\sigma^2}{2^b} + \frac{1}{2^\tau}$$

が成立する．ここで，A_1 の計算時間は $t + O(b\sigma)$ 以下，質問回数は σ 以下である.

定理 5.1 は，E が擬似ランダム置換であれば，CMAC は存在偽造不能性を満たすということを示している．なお，Nandi [30] は，定理 5.1 を改良し，定理 5.1 の式の右辺第二項を $O(\ell q^2/2^b)$ とする結果を与えている．ℓ は最長の質問のメッセージブロック数である．

5.2.2 識別攻撃と偽造攻撃

Jia, Wang, Yuan, Xu は，衝突攻撃を利用して，CBC モードに基づく多くの認証用暗号利用モードに適用可能な識別攻撃および偽造攻撃を提案している [19]．これらの攻撃は，CMAC および，後に述べる ISO/IEC 9797-1 の CBC-MAC の 6 個のアルゴリズムのうち，最初の 4 個に適用可能である．

以下では $\tau = b$ を仮定する．このとき，定理 5.1 は，CMAC に対する E の性質を利用しない攻撃に要するブロック暗号の呼出し回数が $\Omega(2^{b/2})$ であることを示している．以下に示す識別攻撃，偽造攻撃は，E の性質を利用しない攻撃であり，攻撃に必要なブロック暗号の呼出し回数は $O(2^{b/2})$ である．このことから，定理 5.1 より導出された攻撃計算量の下界 $\Omega(2^{b/2})$ が最適であることが分かる．

攻撃アルゴリズムについて記す前に，CBC-MAC に関する表記法を定義する．$M = M_1\|M_2\|\cdots\|M_{n-1}\|M_n$ とし，$1 \le i \le n$ について，$\mathsf{len}(M_i) = b$ とする．$\mathsf{CBC\text{-}MAC}[E_K](M)$ を以下のように定義する．

1. $H_1 = E_K(M_1)$
2. $2 \le i \le n$ について，$H_i = E_K(M_i \oplus H_{i-1})$
3. $H_n = \mathsf{CBC\text{-}MAC}[E_K](M)$ とする．

識別攻撃　以下に記す識別攻撃は次の事実を利用する．

命題 5.2 $M_1, M_2, \ldots, M_n \in \Sigma^b$, $M_1' \in \Sigma^b$ とする．$M_1 \neq M_1'$ ならば，

$$\mathsf{CBC\text{-}MAC}[E_K](M_1\|M_2\|\cdots\|M_n) \neq \mathsf{CBC\text{-}MAC}[E_K](M_1'\|M_2\|\cdots\|M_n)$$

である．

命題 5.2 は E_K が置換であることから容易に証明できる．なお，命題 5.2 の条件を満たす $M_1, M_2, \ldots, M_n \in \Sigma^b$, $M_1' \in \Sigma^b$ について，

$$\mathsf{CMAC}_K(M_1\|M_2\|\cdots\|M_n, b) \neq \mathsf{CMAC}_K(M_1'\|M_2\|\cdots\|M_n, b)$$

も同様に成立する．

識別攻撃は以下のとおりである．オラクルは $\mathsf{CMAC}_K(\cdot, b)$ またはランダム関数である．

1. 適当な $n\,(\ge 2)$ を選び，$M_2, \ldots, M_n$ を定める．
2. $i = 1, 2, \ldots, 2^{(b+1)/2}$ について，$M_1^{(i)}$ を無作為に選択して，オラクルに $M_1^{(i)}\|M_2\|\cdots\|M_n$ を質問し，返答 $T^{(i)}$ を得る．

3. $T^{(1)}, \ldots, T^{(2^{(b+1)/2})}$ がすべて異なれば 1 を出力する．それ以外の場合は 0 を出力する．

この攻撃で，オラクルが $\mathsf{CMAC}_K(\cdot, b)$ であれば，出力は常に 1 である．一方，オラクルがランダム関数であれば，出力が 1 である確率はおよそ $1/\mathrm{e} \approx 0.37$ である．したがって，出力が 1 のとき，オラクルは $\mathsf{CMAC}_K(\cdot, b)$，0 のとき，オラクルはランダム関数と判定すると，オラクルとしてこの二つのいずれかが無作為に選択されるとき，判定が正しい確率はおよそ $1 - 1/(2\mathrm{e}) \approx 0.82$ である．

偽造攻撃　以下に記す偽造攻撃は第二原像攻撃であり，Brincat と Mitchell [8] の攻撃の改良版と位置づけられる．この攻撃は以下の事実を利用する．

命題 5.3 $M_1, M_2, \ldots, M_n \in \Sigma^b$, $M_1', M_2' \in \Sigma^b$ とする．このとき，

$$\begin{gathered}\mathsf{CBC\text{-}MAC}[E_K](M_1 \| M_2 \| M_3 \| \cdots \| M_n) = \mathsf{CBC\text{-}MAC}[E_K](M_1' \| M_2' \| M_3 \| \cdots \| M_n) \\ \Updownarrow \\ E_K(M_1) \oplus M_2 = E_K(M_1') \oplus M_2'\end{gathered}$$

である．

命題 5.3 は $\mathsf{CBC\text{-}MAC}[E_K](\cdot)$ を $\mathsf{CMAC}_K(\cdot, b)$ で置き換えても成立する．命題 5.3 も E_K が置換であることから容易に証明できる．

偽造攻撃は以下のとおりである．オラクルは $\mathsf{CMAC}_K(\cdot, b)$ である．

1. 適当な $n\,(\geq 3)$ を選び，$M_1, M_2, \ldots, M_n$ を定める．
2. $i = 1, 2, \ldots, 2^{(b+1)/2}$ について，$M_1^{(i)}, M_2^{(i)}$ を無作為に選択して，$M_1^{(i)} \| M_2 \| M_3 \| \cdots \| M_n$ と $M_1 \| M_2^{(i)} \| M_3 \| \cdots \| M_n$ とをオラクルに質問し，それぞれに対する返答 $T_1^{(i)}$, $T_2^{(i)}$ を得る．
3. $\{T_1^{(i)} \mid 1 \leq i \leq 2^{(b+1)/2}\}$ と $\{T_2^{(i)} \mid 1 \leq i \leq 2^{(b+1)/2}\}$ との間の衝突を探索する．$T_1^{(i_1)} = T_1^{(i_2)}$ であったとすると，命題 5.3 より，

   $$\begin{aligned} E_K(M_1^{(i_1)}) \oplus M_2 &= E_K(M_1) \oplus M_2^{(i_2)} \\ E_K(M_1) \oplus M_2 &= E_K(M_1^{(i_1)}) \oplus M_2^{(i_2)} \end{aligned}$$

   が導かれる．したがって，$M_1 \| M_2 \| M_3 \| \cdots \| M_n$ と $M_1^{(i_1)} \| M_2^{(i_2)} \| M_3 \| \cdots \| M_n$ の認証子は一致するので，一方の認証子をオラクルへ質問して得ることにより，他方の認証子が得られる．

5.3　まとめ

CMAC は，適応的選択文書攻撃に対する存在偽造不能性，識別不能性を示す証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック

暗号を用いる場合，ブロック暗号のブロック長を b とするとき，攻撃に要するブロック暗号の呼出し回数は $\Theta(2^{b/2})$ であると考えられる．

この結果より，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては，CMAC は安全な認証用暗号利用モードであると言える．なお，偽造攻撃に対する安全性の観点から，$\tau \geq b/2$ とすべきであるということが NIST SP 800-38B にも記されている．

第6章　NIST SP 800-38CのCCM

本章では，NIST SP 800-38C [10] で規定されている守秘・認証用暗号利用モード CCM (Counter with Cipher Block Chaining-Message Authentication Code) の仕様と安全性評価の結果を報告する．CCM は，Whiting, Housley, Ferguson [37] により提案された Authenticated Encryption with Associated Data (AEAD) と呼ばれる共通鍵認証暗号化方式である．CCM は，その名前のとおり，守秘用のカウンタモードと認証用の CBC-MAC を組み合わせた暗号利用モードである．

6.1　仕様

CCM は認証子生成・暗号化アルゴリズム Generation-Encryption と，復号・検証アルゴリズム Decryption-Verification からなる．なお，CCM ではブロック長 128 ビットのブロック暗号を用いるよう規定されている．また，CCM ではブロック暗号の暗号化関数のみが用いられ，復号関数は用いられない．

Generation-Encryption　入力は (N, A, P) であり，N は nonce，A は associated data，P は平文である．出力は暗号文 C である．処理の手順は以下のとおりである．

1. (N, A, P) にフォーマット関数を適用し，$B_0, B_1, \ldots, B_r$ を計算する．
2. $Y_0 = E_K(B_0)$
3. $1 \le i \le r$ について，$Y_i = E_K(B_i \oplus Y_{i-1})$
4. $T = \mathsf{msb}_\tau(Y_r)$
5. カウンタ生成関数を用いて，カウンタブロック $ctr_0, ctr_1, \ldots, ctr_m$ を計算する．ここで，$m = \lceil \mathsf{len}(P)/128 \rceil$ である．
6. $0 \le j \le m$ について，$S_j = E_K(ctr_j)$
7. $S = S_1 \| S_2 \| \cdots \| S_m$
8. $C = (P \oplus \mathsf{msb}_{\mathsf{len}(P)}(S)) \| (T \oplus \mathsf{msb}_\tau(S_0))$

上述のフォーマット関数については以下の性質が要求されている．

- B_0 から N が一意に決まる．

- $B_0, B_1, \ldots, B_r$ から P, A が一意に決まる．さらに，prefix-free であること，すなわち，$(N, P, A) \neq (N', P', A')$ のとき，一方を入力とするフォーマット関数の出力が，他方を入力とするフォーマット関数の出力の接頭辞となることがないこと．
- B_0 は同じ秘密鍵 K を用いた CCM で使用されるどのカウンタブロックとも異なる．

Generation-Encryption の計算手順を図 6.1 に示す．

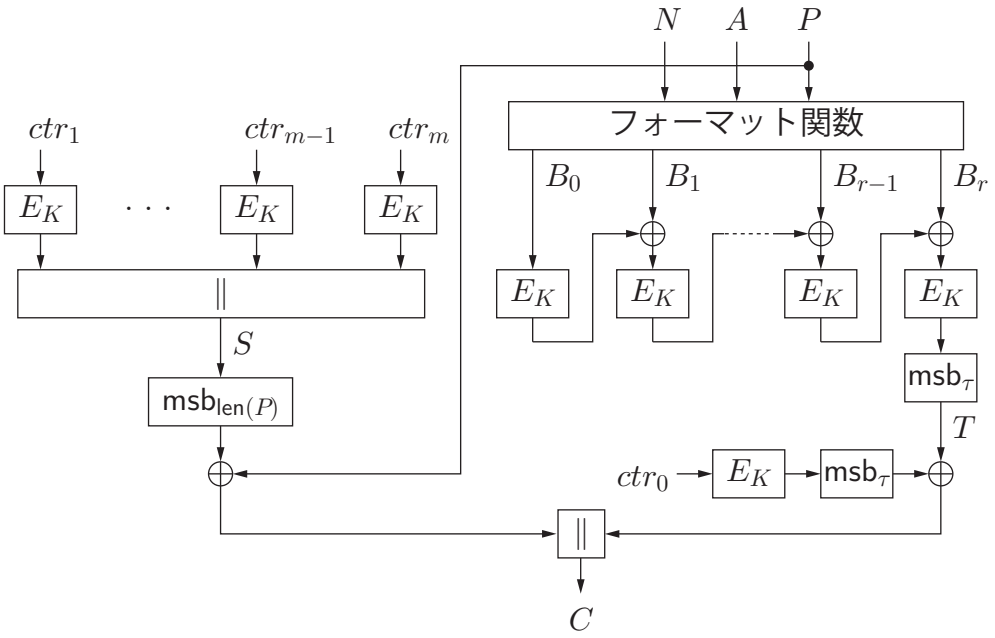


図 6.1: Generation-Encryption の計算手順

Decryption-Verification　入力 (N, A, C) に対する処理の手順は以下のとおりである．

1. $\mathsf{len}(C) \leq \tau$ のとき，`INVALID` を返す．
2. カウンタ生成関数を用いて，カウンタブロック $ctr_0, ctr_1, \ldots, ctr_m$ を計算する．ここで，$m = \lceil (\mathsf{len}(C) - \tau)/128 \rceil$ である．
3. $0 \leq j \leq m$ について，$S_j = E_K(ctr_j)$
4. $S = S_1 \| S_2 \| \cdots \| S_m$
5. $P = \mathsf{msb}_{\mathsf{len}(C)-\tau}(C) \oplus \mathsf{msb}_{\mathsf{len}(C)-\tau}(S)$
6. $T = \mathsf{lsb}_\tau(C) \oplus \mathsf{msb}_\tau(S_0)$
7. (N, A, P) に不備があれば `INVALID` を返す．それ以外の場合，(N, A, P) にフォーマット関数を適用し，$B_0, B_1, \ldots, B_r$ を計算する．
8. $Y_0 = E_K(B_0)$
9. $1 \leq i \leq r$ について，$Y_i = E_K(B_i \oplus Y_{i-1})$

10. $T \neq \mathsf{msb}_\tau(Y_r)$ であれば INVALID を返す．$T = \mathsf{msb}_\tau(Y_r)$ であれば P を返す．

Decryption-Verification の計算手順を図 6.2 に示す．

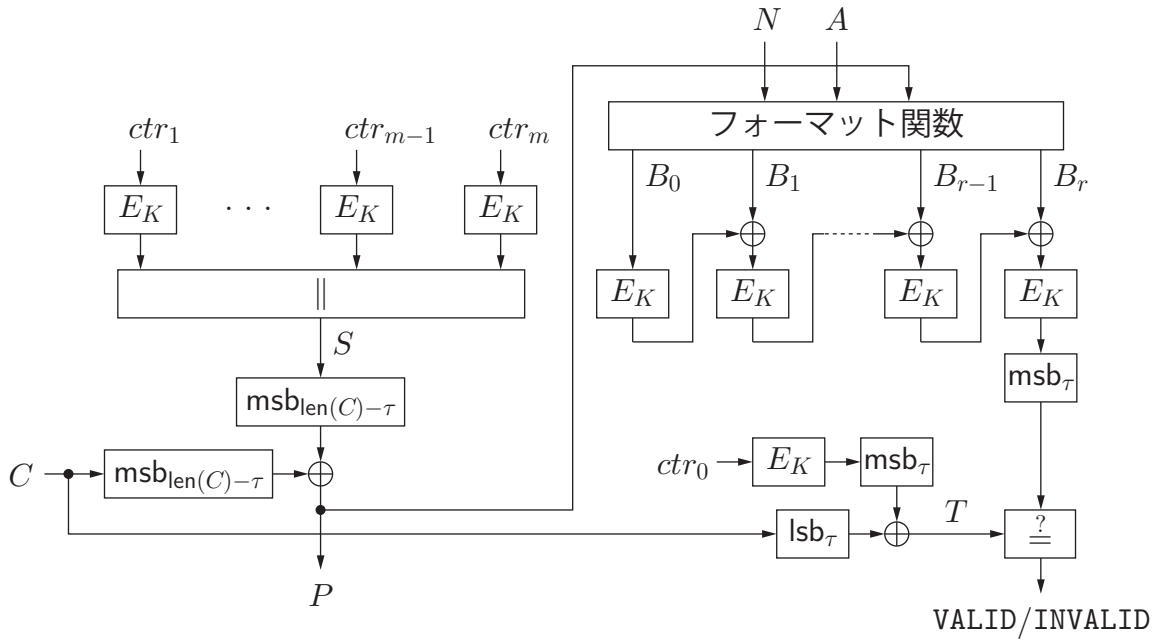


図 6.2: Decryption-Verification の計算手順

6.2 安全性

CCM の証明可能安全性は Jonsson [21] により与えられている．本節ではその結果について記す．以下ではフォーマット関数を β で表す．

偽造不能性は，3.3 節に記した定義よりも強い定義のもとで議論されている．3.3 節の定義では，攻撃者には暗号化オラクルのみが与えられるが，文献 [21] の定義では，攻撃者に対して復号オラクルも与えられる．さらに，復号オラクルには同じ値の nonce を伴う質問を複数回行うことが許可されている．また，復号オラクルへの質問の nonce が，暗号化オラクルへの質問の nonce と同じ値となることも許可されている．

暗号化オラクルに対する質問 $Q = (N, H, M)$ について，

$$l_Q = \left\lceil \frac{\mathsf{len}(\beta(N, H, M)) + \mathsf{len}(M)}{b} \right\rceil + 1$$

と定義する．l_Q は質問 Q の処理に要するブロック暗号の呼出し回数の合計を表す．また，暗号化オラクルに対する質問 $Q^* = (N^*, H^*, C^*)$ について，

$$l_{Q^*} = \left\lceil \frac{\mathsf{len}(\beta(N^*, H^*, M^*)) + \mathsf{len}(C^*)}{b} \right\rceil + 1$$

と定義する．ここで，M^* は Q^* に対応する平文であり，l_{Q^*} は，C^* を復号して Q^* が正しい暗号文かどうかを確認するために必要なブロック暗号の呼出し回数の合計を表す．

Jonsson [21] は偽造不能性に関して以下の定理を示している．

定理 6.1 (定理 1 [21]) A を CCM に対する偽造攻撃者とする．$q_{\mathcal{E}}$ を暗号化オラクルに対する質問回数とし，暗号化オラクルへの質問を $Q_1, Q_2, \ldots, Q_{q_{\mathcal{E}}}$ と表記する．また，$q_{\mathcal{D}}$ を復号オラクルに対する質問回数とし，復号オラクルへの質問を $Q_1^*, Q_2^*, \ldots, Q_{q_{\mathcal{D}}}^*$ と表記する．さらに，

$$l_{\mathcal{E}} = \sum_{i=1}^{q_{\mathcal{E}}} l_{Q_i} \qquad l_{\mathcal{D}} = \sum_{i=1}^{q_{\mathcal{D}}} l_{Q_i^*}$$

と定義する．このとき，E に対するある prp 攻撃者 B が存在して，

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{CCM}}(A) \leq \mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{q_{\mathcal{D}}}{2^{\tau}} + \frac{(l_{\mathcal{E}} + l_{\mathcal{D}})^2}{2^b}$$

が成立する．なお，B の計算時間は，オラクルを利用して A に対する暗号化オラクルと復号オラクルを模倣するのに要する時間と A の計算時間との和であり，B のオラクルへの質問回数は $l_{\mathcal{E}} + l_{\mathcal{D}}$ である．

守秘性は 3.3 節に記した IND$-CPA と同じ定義のもとで議論されており，以下の定理が示されている．

定理 6.2 (定理 2 [21]) A を CCM に対する識別攻撃者とする．$q_{\mathcal{E}}$ を暗号化オラクルに対する質問回数とし，$l_{\mathcal{E}}$ を定理 6.1 と同様に定義する．このとき，E に対するある prp 攻撃者 B が存在して，

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{CCM}}(A) \leq \mathrm{Adv}^{\mathrm{prp}}_{E}(B) + \frac{{l_{\mathcal{E}}}^2}{2^b}$$

が成立する．なお，B の計算時間は，オラクルを利用して A に対する暗号化オラクルを模倣するのに要する時間と A の計算時間との和であり，B のオラクルへの質問回数は $l_{\mathcal{E}}$ である．

Fouque, Martinet, Valette, Zimmer [14] は，CCM で，守秘用のカウンタモードと認証用の CBC-MAC で独立な個別の鍵を用いた場合の証明可能安全性を議論している．彼らは，この方式が選択暗号文攻撃に対して安全であることを述べているが，CCM では，カウンタモードと CBC-MAC で同一の鍵を利用しているため，この結果は CCM には直接適用できない．

6.3 まとめ

CCM は，適応的選択平文攻撃に対する証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合，ブロック暗号のブロック長を b とするとき，攻撃に要するブロック暗号の呼出し回数は $\Theta(2^{b/2})$ であると考えられる．

この結果より，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては，CCM は適応的選択平文攻撃に対して安全な守秘・認証用暗号利用モードであると言える．

第7章　NIST SP 800-38DのGCMとGMAC

本章では，NIST SP 800-38D [12] で規定されているGCMおよびGMACの仕様と安全性評価の結果を報告する．GCMは，CCMと同様，AEADと呼ばれる共通鍵認証暗号化方式である．なお，GCMでは，ブロック長128ビットのブロック暗号を用いるよう規定されている．

7.1　表記法

二値系列 $x \in \Sigma^{128}$ について，

$$\mathsf{inc}_{32}(x) = \mathsf{msb}_{96}(x) \| (\mathsf{lsb}_{32}(x) + 1 \bmod 2^{32})$$

と定義する．また，非負整数 a について，a の64ビット二進数表記を $[a]_{64}$ で表す．

7.2　仕様

GCMはブロック暗号のカウンタモードによる暗号化関数と，ユニバーサルハッシュ関数を利用したメッセージ認証コードからなる．

GCMで用いられるユニバーサルハッシュ関数 $\mathsf{GHASH}_H(X)$ は以下のとおりである．なお，$X = X_1 \| X_2 \| \cdots \| X_m$ とし，$1 \le i \le m$ について，X_i の長さは128ビットとする．すなわち，X の長さは128の倍数である．加算と乗算は $\mathrm{GF}(2^{128})$ の演算である．GCMでは法として $\mathtt{u}^{128} + \mathtt{u}^7 + \mathtt{u}^2 + \mathtt{u} + 1$ が用いられている．

1. $Y_0 = 0$
2. $1 \le i \le m$ について，$Y_i = (Y_{i-1} \oplus X_i) \cdot H$ とする．
3. Y_m を出力する．

これより，

$$\mathsf{GHASH}_H(X) = X_1 \cdot H^m \oplus X_2 \cdot H^{m-1} \oplus \cdots \oplus X_{m-1} \cdot H^2 \oplus X_m \cdot H$$

である．$\mathsf{GHASH}_H(X)$ を図7.1に示す．

GCMで用いられるブロック暗号を E とし，E のブロック長を128とする．GCMのカウンタモードによる暗号化アルゴリズム $\mathsf{GCTR}_K(ICB, X)$ は以下のとおりである．なお，$X = X_1 \| X_2 \| \cdots \| X_{n-1} \| X_n^*$ とし，$1 \le i \le n-1$ について，$\mathsf{len}(X_i) = 128$，$1 \le \mathsf{len}(X_n^*) \le 128$ とする．ここで，$n = \lceil \mathsf{len}(X)/128 \rceil$ である．また，$ICB \in \{0,1\}^{128}$ である．

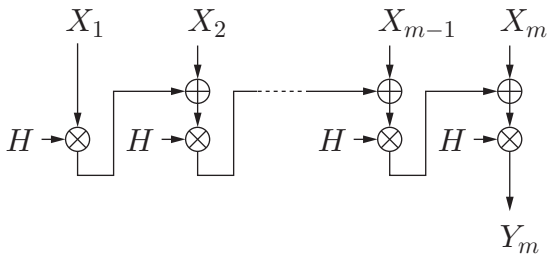


図 7.1: $\mathsf{GHASH}_H(X)$

1. X が空列であれば，空列 Y を出力する．
2. $CB_1 = ICB$ とし，$2 \le i \le n$ について，$CB_i = \mathsf{inc}_{32}(CB_{i-1})$ とする．
3. $1 \le i \le n-1$ について，$Y_i = X_i \oplus E_K(CB_i)$
4. $Y_n^* = X_n^* \oplus \mathsf{msb}_{\mathsf{len}(X_n^*)}(E_K(CB_n))$
5. $Y = Y_1 \| Y_2 \| \cdots \| Y_{n-1} \| Y_n^*$ を出力する．

$\mathsf{GCTR}_K(ICB, X)$ を図 7.2 に示す．

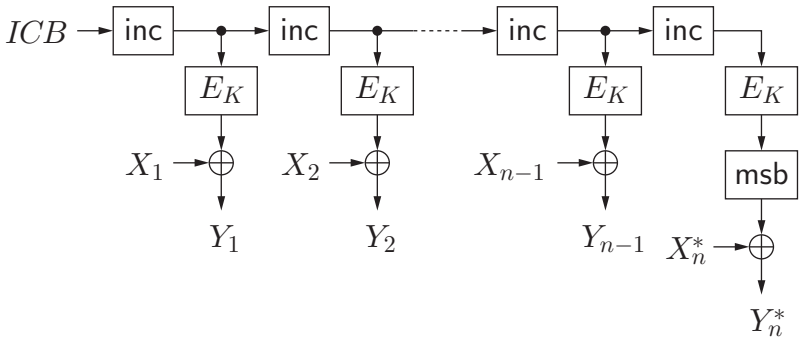


図 7.2: $\mathsf{GCTR}_K(ICB, X)$．inc は inc_{32} を表す．msb は $\mathsf{msb}_{\mathsf{len}(X_n^*)}$ を表す．

以下に GCM の認証付暗号化および認証付復号のアルゴリズムを記す．なお，これらのアルゴリズムで，平文 P，暗号文 C が空列の場合が，GMAC の MAC 生成と検証のアルゴリズムとなる．

認証付暗号化　GCM の認証付暗号化アルゴリズム $\mathsf{GCM\text{-}AE}_K(IV, P, A)$ は GCTR, GHASH を用いて以下のように定義される．IV は初期値であり，$1 \le |IV| \le 2^{64} - 1$ である．P は平文であり，$0 \le \mathsf{len}(P) \le (2^{32} - 2) \times 128$ である．A は associated data であり，$0 \le \mathsf{len}(A) \le 2^{64} - 1$ である．

1. $H = E_K(0^{128})$
2. J_0 を以下のように定める．

$$J_0 = \begin{cases} IV \| 0^{31}1 & (\mathsf{len}(IV) = 96) \\ \mathsf{GHASH}_H(IV \| 0^{s+64} \| [\mathsf{len}(IV)]_{64}) & (\mathsf{len}(IV) \ne 96). \end{cases}$$

ここで，$s = 128\lceil \mathsf{len}(IV)/128 \rceil - \mathsf{len}(IV)$ である．

3. $C = \mathsf{GCTR}_K(\mathsf{inc}_{32}(J_0), P)$
4. S を以下のように定める．

$$S = \mathsf{GHASH}_H(A \| 0^v \| C \| 0^u \| [\mathsf{len}(A)]_{64} \| [\mathsf{len}(C)]_{64}).$$

ここで

$$u = 128\lceil \mathsf{len}(C)/128 \rceil - \mathsf{len}(C)$$
$$v = 128\lceil \mathsf{len}(A)/128 \rceil - \mathsf{len}(A)$$

である．

5. $T = \mathsf{msb}_\tau(\mathsf{GCTR}_K(J_0, S))$
6. (C, T) を出力する．

$\mathsf{GCM\text{-}AE}_K(IV, P, A)$ を図 7.3 に示す．

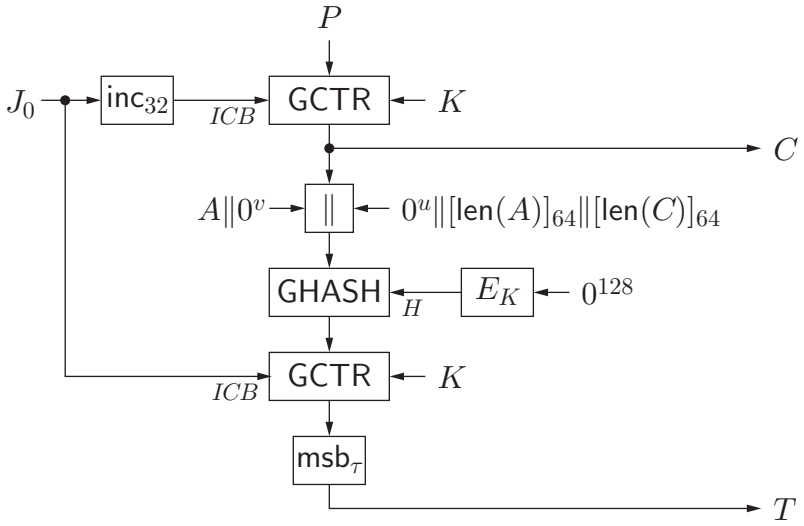


図 7.3: $\mathsf{GCM\text{-}AE}_K(IV, P, A)$

認証付復号　GCM の認証付復号アルゴリズム $\mathsf{GCM\text{-}AD}_K(IV, C, A, T)$ は以下のように定義される．

1. IV, C, A のビット長が定義の範囲外であるか，あるいは，$\mathsf{len}(T) \neq \tau$ のとき，`INVALID` を返す．
2. $H = E_K(0^{128})$

3. J_0 を以下のように定める．

$$J_0 = \begin{cases} IV \| 0^{31}1 & (\mathsf{len}(IV) = 96) \\ \mathsf{GHASH}_H(IV \| 0^{s+64} \| [\mathsf{len}(IV)]_{64}) & (\mathsf{len}(IV) \neq 96). \end{cases}$$

ここで，$s = 128\lceil \mathsf{len}(IV)/128 \rceil - \mathsf{len}(IV)$ である．

4. $P = \mathsf{GCTR}_K(\mathsf{inc}_{32}(J_0), C)$

5. S を以下のように定める．

$$S = \mathsf{GHASH}_H(A \| 0^v \| C \| 0^u \| [\mathsf{len}(A)]_{64} \| [\mathsf{len}(C)]_{64}).$$

ここで

$$u = 128\lceil \mathsf{len}(C)/128 \rceil - \mathsf{len}(C)$$
$$v = 128\lceil \mathsf{len}(A)/128 \rceil - \mathsf{len}(A)$$

である．

6. $T' = \mathsf{msb}_\tau(\mathsf{GCTR}_K(J_0, S))$

7. $T = T'$ であれば，P を出力する．$T \neq T'$ であれば，`INVALID` を出力する．

$\mathsf{GCM\text{-}AD}_K(IV, C, A, T)$ における P, T' の計算手順を図 7.4 に示す．

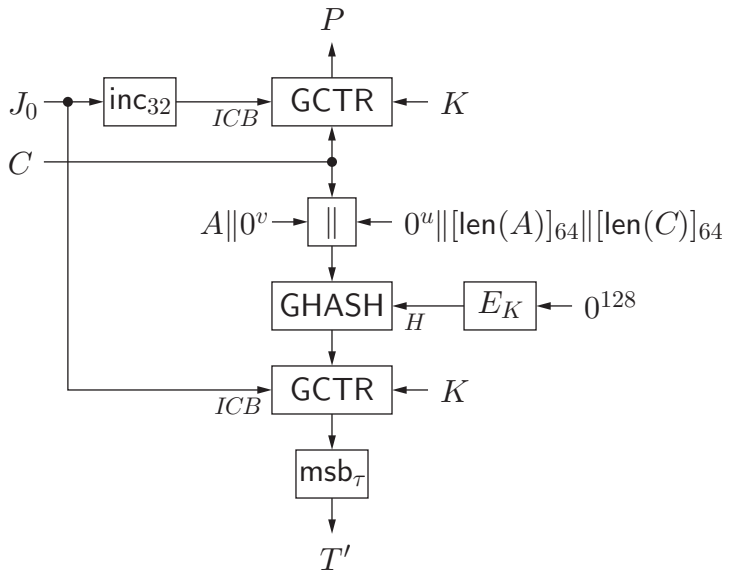


図 7.4: $\mathsf{GCM\text{-}AD}_K(IV, C, A, T)$ における P, T' の計算手順

7.3 安全性

GCM の証明可能安全性は，提案者の McGrew と Viega により論じられている [27, 28].

McGrew と Viega は，[36, 34] の AEAD の安全性定義に基づいて，GCM の安全性を定義している．守秘性の定義では，攻撃者は，暗号化オラクルと復号オラクルを有する．暗号化オラクルは，IV, A, P を受け取り，C, T を返す．復号オラクルは，IV, A, C, T を受け取り，P または INVALID を返す．なお，攻撃者は各オラクルに対して同じ nonce (IV) を用いた質問を行わないと仮定される．ただし，暗号化オラクルと復号オラクルに，それぞれ 1 回ずつ同じ nonce を用いた質問を行うことは許される．

定理 7.1 (定理 1 [28]) GCM の暗号化関数とランダム関数とを優位度 α_{GCM} で識別する攻撃者が存在すると仮定する．攻撃者の質問回数を q 以下，質問の平文の総長を ℓ_{P} ビット以下，各質問について，$\mathsf{len}(C) + \mathsf{len}(A) \leq \ell, \mathsf{len}(IV) \leq \ell_{\mathrm{IV}}$ とする．このとき，E とランダム置換とを優位度 α_E で識別する攻撃者が存在して，

$$\alpha_{\mathrm{GCM}} \leq \alpha_E + \frac{(\ell_{\mathrm{P}}/b + 2q)^2}{2^{b+1}} + \frac{2q(\ell_{\mathrm{P}}/b + 2q)\lceil \ell_{\mathrm{IV}}/b + 1 \rceil}{2^b} + \frac{q\lceil \ell/b + 1 \rceil}{2^\tau}$$

が成立する．

定理 7.2 (定理 2 [28]) GCM に対して，β_{GCM} で偽造に成功する攻撃者が存在すると仮定する．この攻撃者の質問回数を q 以下，質問の平文の総長を ℓ_{P} ビット以下，各質問について，$\mathsf{len}(C) + \mathsf{len}(A) \leq \ell, \mathsf{len}(IV) \leq \ell_{\mathrm{IV}}$ とする．このとき，E とランダム置換とを優位度 α_E で識別する攻撃者が存在して，

$$\beta_{\mathrm{GCM}} \leq \alpha_E + \frac{(\ell_{\mathrm{P}}/b + 2q)^2}{2^{b+1}} + \frac{2q(\ell_{\mathrm{P}}/b + 2q + 1)\lceil \ell_{\mathrm{IV}}/b + 1 \rceil}{2^b} + \frac{q\lceil \ell/b + 1 \rceil}{2^\tau}$$

が成立する．

McGrew と Viega は，上記の定理を IPsec 用の AES を用いた GCM に適用した結果について述べている [27, 28]．彼らは，$\ell_{IV} = 96, \tau = 96$ とし，さらに，パケットの最大長として 1500 バイトを仮定し，$\ell \leq 12000$ としている．また，AES については，ブロック長 $b = 128$ であり，鍵長 κ の AES を AES-κ と表記する．

系 7.3 AES-κ に対するランダム置換との識別に関する優位度が $\alpha_{\text{AES-}\kappa}$ より大きな攻撃が存在せず，高々 q 個のパケットが処理されると仮定する．このとき，AES-κ を用いた GCM に対して以下が成立する．

- $\alpha_{\text{AES-}\kappa} + q^2/2^{116} - q/2^{89.4}$ より大きな優位度を有する識別攻撃は存在しない．
- $\alpha_{\text{AES-}\kappa} + q^2/2^{116} - q/2^{89.4} - q/2^{128}$ より大きな優位度を有する偽造攻撃は存在しない．

7.4 まとめ

GCM は適応的選択暗号文攻撃に対する証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては，GCM は適応的選択暗号文攻撃に対して安全な守秘・認証用暗号利用モードであると言える．

また，GCM に関する証明可能安全性の結果より，GMAC は適応的選択文書攻撃に対する証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては，GMAC は適応的選択文書攻撃に対して安全な認証用暗号利用モードであると言える．

ただし，証明可能安全性に関する攻撃者の優位度の上界は，初期値 IV の長さ等も含めた多数のパラメータに依存するため，個別のケースに関して，系 7.3 に示されているような解析が重要である．

第8章　ISO/IEC 9797-1の CBC-MAC

本章では，ISO/IEC 9797-1:1999 [16] で規定されている MAC アルゴリズムの仕様と安全性評価の結果を報告する．

8.1　仕様

ISO/IEC 9797-1:1999 では，6 個の MAC アルゴリズムが規定されている．これらのアルゴリズムでは，入力メッセージの長さは b の倍数であることが仮定されている．なお，入力メッセージの長さが b の倍数でない場合に関して，ISO/IEC 9797-1:1999 では，三つのパディング法が規定されている．以下では，$M = M_1 \| M_2 \| \cdots \| M_{n-1} \| M_n$ とし，$1 \leq i \leq n$ について，$\mathsf{len}(M_i) = b$ とする．

8.1.1　アルゴリズム 1

このアルゴリズムでは一つの秘密鍵 K が用いられる．メッセージ M に対する認証子 T は

$$T = \mathsf{msb}_\tau(\mathsf{CBC\text{-}MAC}[E_K](M))$$

である．アルゴリズム 1 を図 8.1 に示す．

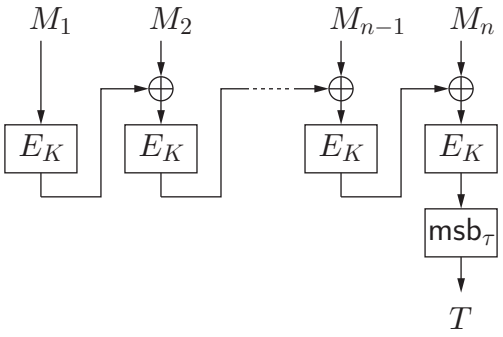


図 8.1: アルゴリズム 1

8.1.2 アルゴリズム 2

このアルゴリズムでは二つの秘密鍵 K, K''' が用いられる．メッセージ M に対する認証子は

$$T = \mathsf{msb}_\tau(E_{K'''}(\mathsf{CBC\text{-}MAC}[E_K](M)))$$

である．アルゴリズム 2 を図 8.2 に示す．

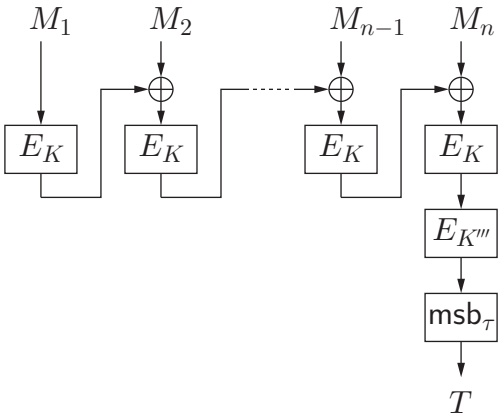


図 8.2: アルゴリズム 2

8.1.3 アルゴリズム 3

このアルゴリズムでは二つの秘密鍵 K, K' が用いられる．メッセージ M に対する認証子は

$$T = \mathsf{msb}_\tau(E_K(D_{K'}(\mathsf{CBC\text{-}MAC}[E_K](M))))$$

である．アルゴリズム 3 を図 8.3 に示す．

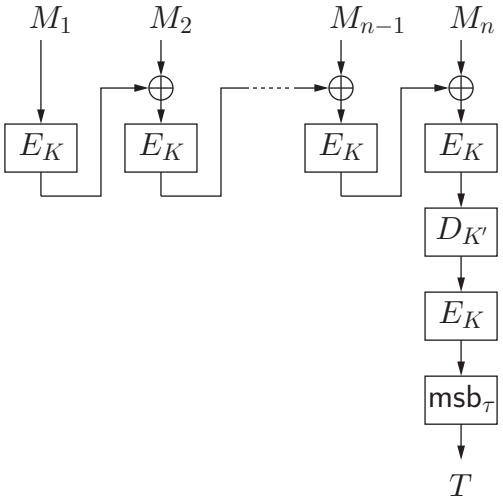


図 8.3: アルゴリズム 3

8.1.4 アルゴリズム 4

このアルゴリズムでは，独立に選択される二つの秘密鍵 K, K' が用いられる．さらに，三つ目の秘密鍵 K'' が K' から導出される．メッセージ M に対する認証子 T は以下のように計算される．

1. $H_1 = E_{K''}(E_K(M_1))$
2. $2 \leq i \leq n$ について，$H_i = E_K(M_i \oplus H_{i-1})$
3. $T = \mathsf{msb}_\tau(E_K(D_{K'}(H_n)))$ とする．

アルゴリズム 4 を図 8.4 に示す．

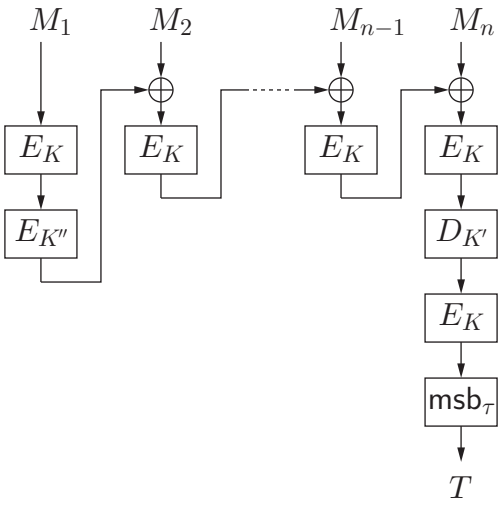


図 8.4: アルゴリズム 4

8.1.5 アルゴリズム 5

このアルゴリズムでは，一つの秘密鍵 K から相異なる二つの秘密鍵 K_1, K_2 を導出して用いる．認証子の計算法は以下のとおりである．

1. K_1 を用いてアルゴリズム 1 により T_1 を計算する．
2. K_2 を用いてアルゴリズム 1 により T_2 を計算する．
3. $T = T_1 \oplus T_2$ を出力する．

したがって，メッセージ M に対する認証子は

$$T = \mathsf{msb}_\tau(\mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus \mathsf{CBC\text{-}MAC}[E_{K_2}](M))$$

である．

8.1.6 アルゴリズム 6

このアルゴリズムでは，独立に選択される二つの秘密鍵 K, K' が用いられる．このアルゴリズムではまず，(K, K') から，以下を満たすように $(K_1, K_1'), (K_2, K_2')$ が導出される．

$$K_1 \neq K_1', \quad K_2 \neq K_2', \quad (K_1, K_1') \neq (K_2, K_2')$$

認証子の計算法は以下のとおりである．

1. (K_1, K_1') を用いてアルゴリズム 4 により T_1 を計算する．
2. (K_2, K_2') を用いてアルゴリズム 4 により T_2 を計算する．
3. $T = T_1 \oplus T_2$ を出力する．

8.2 安全性

8.2.1 アルゴリズム 1

証明可能安全性

アルゴリズム 1 の証明可能安全性に関しては，Petrank と Rackoff [32] や Bellare, Pietrzak, Rogaway[7] により議論されている．なお，アルゴリズム 1 に関しては，メッセージ空間は prefix-free であることを仮定する．すなわち，任意の二つの異なるメッセージについて，それらは互いに他方の接頭辞になることはないと仮定する．

アルゴリズム 1 の E_K を一様分布に基づいて選択された Σ^b 上の置換に置き換えて得られる関数と真のランダム関数との識別不能性に関して以下の結果が示されている [32, 7]．

補題 8.1 ([32]) B を $\mathcal{F}((\Sigma^b)^+, \Sigma^b)$ の関数をオラクルとする攻撃者とする．B のオラクルへの質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，

$$\Pr[B^{\mathsf{CBC\text{-}MAC}[\pi]} = 1] - \Pr[B^{\rho} = 1] \leq \frac{13\sigma^2}{2^{b+1}}$$

が成立する．ここで，π は $\mathcal{P}(\Sigma^b)$ 上の一様分布に基づく独立な確率変数であり，ρ は $\mathcal{F}(\mathcal{M}, \Sigma^b)$ 上の一様分布に基づく確率変数である．なお，$\mathcal{M} \subset (\Sigma^b)^{\leq m}$ は，prefix-free メッセージ空間であり，m は，B の一つの質問に含まれるメッセージブロック数の最大値である．

補題 8.2 (定理 1 [7]) B を $\mathcal{F}((\Sigma^b)^+, \Sigma^b)$ の関数をオラクルとする攻撃者とする．B のオラクルへの質問回数を q 以下，最も長い質問に含まれるメッセージブロックの個数を m 以下とする．$m \leq 2^{b/2-1}$ のとき，

$$\Pr[B^{\mathsf{CBC\text{-}MAC}[\pi]} = 1] - \Pr[B^{\rho} = 1] \leq \frac{mq^2}{2^b}\left(12 + \frac{8m^3}{2^b}\right)$$

が成立する．ここで，π は $\mathcal{P}(\Sigma^b)$ 上の一様分布に基づく確率変数であり，ρ は $\mathcal{F}(\mathcal{M}, \Sigma^b)$ 上の一様分布に基づく確率変数である．なお，$\mathcal{M} \subset (\Sigma^b)^{\leq m}$ は，prefix-free メッセージ空間である．

質問回数が q 以下で，質問に含まれるメッセージブロックの総数が σ 以下の攻撃者 B について，

$$\mathrm{adv}^{\mathrm{prf}}_{\mathsf{CBC\text{-}MAC}[\pi]}(b,q,\sigma) \stackrel{\mathrm{def}}{=} \max_{B} \left\{ \Pr[B^{\mathsf{CBC\text{-}MAC}[\pi]} = 1] - \Pr[B^{\rho} = 1] \right\}$$

と定義する．これを用いると，アルゴリズム 1 の偽造不能性に関して以下の定理が導かれる．

定理 8.3 A をアルゴリズム 1 に対する偽造攻撃者とする．A の計算時間を t 以下，オラクルへの質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，以下を満たす E に対する prf 攻撃者 A' が存在する．

$$\mathrm{Adv}^{\mathrm{mac}}_{\mathrm{alg1}}(A) \leq \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \mathrm{adv}^{\mathrm{prf}}_{\mathsf{CBC\text{-}MAC}[\pi]}(b,q,\sigma) + \frac{1}{2^{\tau}}$$

ここで，A' の計算時間は $t + O(b\sigma)$ 以下，質問回数は σ 以下である．

識別攻撃と偽造攻撃

アルゴリズム 1 には，5.2 節に記した Jia, Wang, Yuan, Xu による識別攻撃および偽造攻撃 [19] が適用可能である．これらの攻撃に要するブロック暗号の呼出し回数は $O(2^{b/2})$ である．

8.2.2 アルゴリズム 2

証明可能安全性

アルゴリズム 2 に関しては，Petrank と Rackoff [32] や Bellare, Pietrzak, Rogaway[7] により証明可能安全性が議論されている．アルゴリズム 2 の E_K と $E_{K'''}$ を一様かつ独立に選択された二つの置換に置き換えて得られる関数と真のランダム関数との識別不能性に関して以下の結果が示されている [32, 7].

補題 8.4 (補題 3.3 [32]) B を $\mathcal{F}((\Sigma^b)^+, \Sigma^b)$ の関数をオラクルとする攻撃者とする．B のオラクルへの質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，

$$\Pr[B^{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]} = 1] - \Pr[B^{\rho} = 1] \leq \frac{5\sigma^2}{2^{b+1}}$$

が成立する．ここで，π_1, π_2 は $\mathcal{P}(\Sigma^b)$ 上の一様分布に基づく独立な確率変数であり，ρ は $\mathcal{F}((\Sigma^b)^{\leq m}, \Sigma^b)$ 上の一様分布に基づく確率変数である．なお，m は，B の一つの質問に含まれるメッセージブロック数の最大値である．

補題 8.5 (定理 2 [7]) B を $\mathcal{F}((\Sigma^b)^+, \Sigma^b)$ の関数をオラクルとする攻撃者とする．B のオラクルへの質問回数を q 以下，最も長い質問に含まれるメッセージブロックの個数を m 以下とする．$m \leq 2^{b/2-1}$ のとき，

$$\Pr[B^{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]} = 1] - \Pr[B^{\rho} = 1] \leq \frac{q^2}{2^b}\left(d'(m) + \frac{4m^4}{2^b}\right)$$

が成立する．ここで，π_1, π_2 は $\mathcal{P}(\Sigma^b)$ 上の一様分布に基づく独立な確率変数であり，ρ は $\mathcal{F}((\Sigma^b)^{\leq m}, \Sigma^b)$ 上の一様分布に基づく確率変数である．また，$d'(m)$ は $1 \leq m' \leq m$ なる m' の約数の個数の最大値である．

質問回数が q 以下で，質問に含まれるメッセージブロックの総数が σ 以下の攻撃者 B について，

$$\mathrm{adv}^{\mathrm{prf}}_{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]}(b, q, \sigma) \stackrel{\mathrm{def}}{=} \max_B \left\{\Pr[B^{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]} = 1] - \Pr[B^{\rho} = 1]\right\}$$

と定義する．これを用いると，アルゴリズム 2 の偽造不能性に関して以下の定理が導かれる．

定理 8.6 A をアルゴリズム 2 に対する偽造攻撃者とする．A の計算時間を t 以下，オラクルへの質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，以下を満たす E に対する prf 攻撃者 A' が存在する．

$$\mathrm{Adv}^{\mathrm{mac}}_{\mathrm{alg2}}(A) \leq 2\,\mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \mathrm{adv}^{\mathrm{prf}}_{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]}(b, q, \sigma) + \frac{1}{2^\tau}$$

ここで，A' の計算時間は $t + O(b\sigma)$ 以下，質問回数は σ 以下である．

識別攻撃と偽造攻撃

アルゴリズム 2 には，5.2 節に記した Jia, Wang, Yuan, Xu による識別攻撃および偽造攻撃 [19] が適用可能である．これらの攻撃に要するブロック暗号の呼出し回数は $O(2^{b/2})$ である．

8.2.3 アルゴリズム 3

証明可能安全性

一様かつ独立に選択された Σ^b 上の二つの置換 π_1, π_2 を考える．アルゴリズム 3 の E_K と $D_{K'}$ を π_1, π_2 に置き換えて得られる関数は，

$$\pi_1 \circ \pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]$$

である．ここで，$\pi_1 \circ \pi_2$ は，一様かつ π_1 と独立に選択された一つの置換とみなすことができる．したがって，アルゴリズム 3 の証明可能安全性に関しては，アルゴリズム 2 の議論がほぼそのまま適用できる．

アルゴリズム 3 の偽造不能性に関して以下の定理が導かれる．

定理 8.7 A をアルゴリズム 3 に対する偽造攻撃者とする．A の計算時間を t 以下，オラクルへの質問回数を q 以下，質問に含まれるメッセージブロックの総数を σ 以下とする．このとき，以下を満たす E に対する prp 攻撃者 A_E と D に対する prp 攻撃者 A_D とが存在する．

$$\mathrm{Adv}^{\mathrm{mac}}_{\mathrm{alg3}}(A) \leq \mathrm{Adv}^{\mathrm{prp}}_{E}(A_E) + \mathrm{Adv}^{\mathrm{prp}}_{D}(A_D) + \mathrm{adv}^{\mathrm{prf}}_{\pi_2 \circ \mathsf{CBC\text{-}MAC}[\pi_1]}(b, q, \sigma) + \frac{1}{2^{\tau}}$$

ここで，A_E, A_D の計算時間はともに $t + O(b\sigma)$ 以下，質問回数はともに σ 以下である．

識別攻撃と偽造攻撃

アルゴリズム 3 には，5.2 節に記した Jia, Wang, Yuan, Xu による識別攻撃および偽造攻撃 [19] が適用可能である．これらの攻撃に要するブロック暗号の呼出し回数は $O(2^{b/2})$ である．

8.2.4 アルゴリズム 4

証明可能安全性

アルゴリズム 3 の証明と同様の手法により，アルゴリズム 4 に関しても，ブロック暗号の性質を利用しない識別攻撃に要するブロック暗号の呼出し回数は $\Omega(2^{b/2})$ であることが示せる．

識別攻撃と偽造攻撃

アルゴリズム 4 には，5.2 節に記した Jia, Wang, Yuan, Xu による識別攻撃および偽造攻撃 [19] が適用可能である．これらの攻撃に要するブロック暗号の呼出し回数は $O(2^{b/2})$ である．

8.2.5 アルゴリズム 5

偽造攻撃

アルゴリズム 5 に関しては，Joux, Poupard, Stern [23] により，ブロック暗号の呼出し回数が $O(2^{b/2})$ の偽造攻撃が提案されている．この攻撃法を以下に記す．

1. アルゴリズム 5 について，認証子の一致する相異なるメッセージ M, M' を求める．M, M' のそれぞれの長さは任意で良い．

$$\begin{aligned} &\mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus \mathsf{CBC\text{-}MAC}[E_{K_2}](M) \\ =\ &\mathsf{CBC\text{-}MAC}[E_{K_1}](M') \oplus \mathsf{CBC\text{-}MAC}[E_{K_2}](M') \end{aligned}$$

が成立するので，

$$\begin{aligned}\delta &\stackrel{\text{def}}{=} \mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus \mathsf{CBC\text{-}MAC}[E_{K_1}](M') \\ &= \mathsf{CBC\text{-}MAC}[E_{K_2}](M) \oplus \mathsf{CBC\text{-}MAC}[E_{K_2}](M')\end{aligned}$$

とする．

2. $N, N' \in \Sigma^b$ をそれぞれ $2^{b/2}$ 個ずつ無作為に選び，アルゴリズム 5 による $M\|N$, $M'\|N'$ の認証子を得る．

   ある N, N' について，$N \oplus N' = \delta$ ならば，

$$\begin{aligned}\mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus N &= \mathsf{CBC\text{-}MAC}[E_{K_1}](M') \oplus N' \\ \mathsf{CBC\text{-}MAC}[E_{K_2}](M) \oplus N &= \mathsf{CBC\text{-}MAC}[E_{K_2}](M') \oplus N'\end{aligned}$$

   が成立し，$M\|N$ と $M'\|N'$ の認証子は一致する．さらに，

$$\begin{aligned}\mathsf{CBC\text{-}MAC}[E_{K_1}](M\|N) &= \mathsf{CBC\text{-}MAC}[E_{K_1}](M'\|N') \\ \mathsf{CBC\text{-}MAC}[E_{K_2}](M\|N) &= \mathsf{CBC\text{-}MAC}[E_{K_2}](M'\|N')\end{aligned}$$

   が成立するので，任意の $P \in (\Sigma^b)^+$ について，$M\|N\|P$ と $M'\|N'\|P$ の認証子は一致する．したがって，$M\|N\|P$ の認証子が得られれば，$M'\|N'\|P$ の認証子が偽造できたことになる．

上記のステップ 1 に要するブロック暗号の呼出し回数は明らかに $O(2^{b/2})$ である．

一方，ステップ 2 に関しては，以下の事実に注意すれば，同じく，ブロック暗号の呼出し回数が $O(2^{b/2})$ で，$N \oplus N' = \delta$ を満たす N, N' が得られることが判る．

まず，相異なるメッセージ M, M' を任意に定め，

$$\mathsf{CBC\text{-}MAC}[E_{K_1}](M\|N) = \mathsf{CBC\text{-}MAC}[E_{K_1}](M'\|N')$$

を満たす $N, N' \in \Sigma^b$ を得る．これに要するブロック暗号の呼出し回数は $O(2^{b/2})$ である．このような，N, N' について，

$$E_{K_1}(\mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus N) = E_{K_1}(\mathsf{CBC\text{-}MAC}[E_{K_1}](M') \oplus N')$$

で，E_{K_1} は置換なので，

$$\begin{aligned}\mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus N &= \mathsf{CBC\text{-}MAC}[E_{K_1}](M') \oplus N' \\ N \oplus N' &= \mathsf{CBC\text{-}MAC}[E_{K_1}](M) \oplus \mathsf{CBC\text{-}MAC}[E_{K_1}](M')\end{aligned}$$

が成立する．

8.2.6 アルゴリズム 6

証明可能安全性

安田は，アルゴリズム 6 と類似したアルゴリズム SUM-ECBC を提案し，その安全性解析を行っている [38].

SUM-ECBC は以下のように定義される.

1. $V = \mathsf{CBC\text{-}MAC}[E_{K_1}](M)$
2. $W = \mathsf{CBC\text{-}MAC}[E_{K_3}](M)$
3. $T = E_{K_2}(V) \oplus E_{K_4}(W)$ を出力する.

SUM-ECBC を図 8.5 に示す.

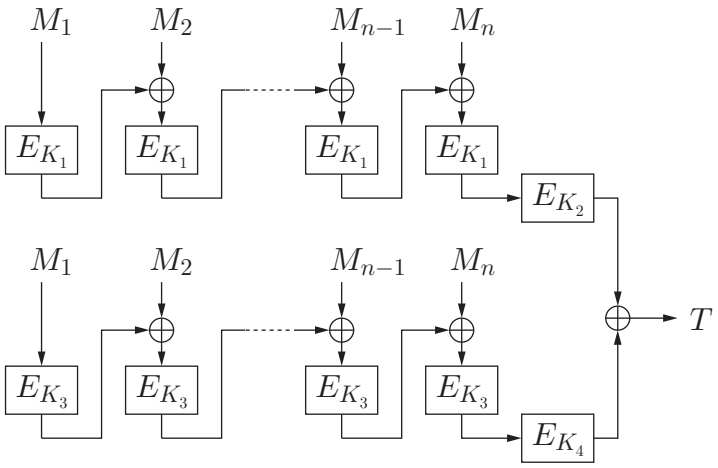


図 8.5: SUM-ECBC

定理 8.8 A を SUM-ECBC に対する prf 攻撃者とする．A の計算時間は t 以下，質問回数は q 以下とする．さらに，各質問のメッセージブロックの個数は ℓ 以下であるとする．このとき，E に対するある prp 攻撃者 A' が存在して，

$$\mathrm{Adv}^{\mathrm{prf}}_{\mathsf{SUM\text{-}ECBC}}(A) \le 4 \cdot \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \frac{12\ell^4 q^3}{2^{2b}}$$

が成立する．特に，$\ell \le 2^{2b/5}$ のとき

$$\mathrm{Adv}^{\mathrm{prf}}_{\mathsf{SUM\text{-}ECBC}}(A) \le 4 \cdot \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \frac{40\ell^3 q^3}{2^{2b}}$$

が成立する．ここで，A' の計算時間は $t + O(\ell q T_E)$ 以下，質問回数は ℓq 以下である．T_E は E の 1 回の計算に要する時間である.

定理 8.8 より，ブロック暗号の性質を利用しない識別攻撃に要するブロック暗号の呼出し回数は $\Omega(2^{2b/3})$ であることが判る．また，定理 8.8 の証明と同様の手法により，アルゴリズム 6 に関しても，ブロック暗号の性質を利用しない識別攻撃に要するブロック暗号の呼出し回数は $\Omega(2^{2b/3})$ であることが示せる [38]．なお，SUM-ECBC，アルゴリズム 6 に対して，ブロック暗号の性質を利用しない呼出し回数が $O(2^{2b/3})$ の識別攻撃が存在するかどうかは未解決問題である.

8.3 まとめ

アルゴリズム 1, 2, 3, 4 は，適応的選択文書攻撃に対する存在偽造不能性，識別不能性に関する証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合，ブロック暗号のブロック長を b とするとき，攻撃に要するブロック暗号の呼出し回数は $\Theta(2^{b/2})$ であると考えられる．ただし，アルゴリズム 1 に関しては，入力メッセージが prefix-free でなければならない．

アルゴリズム 5 に関しては，ブロック暗号の呼出し回数が $\Theta(2^{b/2})$ の偽造攻撃が存在する．一方，証明可能安全性は示されておらず，より効率の良い攻撃が存在するかどうかは未解決問題である．

アルゴリズム 6 は，適応的選択文書攻撃に対する存在偽造不能性，識別不能性に関する証明可能安全性を有しており，AES など，実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合，攻撃に要するブロック暗号の呼出し回数は $\Omega(2^{2b/3})$ であると考えられる．

なお，すべてのアルゴリズムに関して，偽造不能性の観点から，認証子の長さは $\tau \geq b/2$ とすべきである．アルゴリズム 6 に関しては $\tau \geq 2b/3$ とすることが望ましい．

第9章　NIST FIPS 198-1のHMAC

9.1　仕様

HMAC [3] はハッシュ関数を用いて構成されるメッセージ認証コード (MAC: Message Authentication Code) 関数であり，NIST の FIPS PUB 198-1 [31] に規定されている．HMAC はまた擬似ランダム関数として利用される．

ハッシュ関数を H，秘密鍵を K とし，メッセージを M とする．HMAC では通常，H は反復形ハッシュ関数であると仮定される．H の圧縮関数のメッセージブロックの入力長を B バイトとし，出力長を L バイトとする．HMAC は

$$H((K_0 \oplus \mathtt{opad}) \| H((K_0 \oplus \mathtt{ipad}) \| M))$$

と定義される．ここで，

$$K_0 = \begin{cases} K \| 0^{8B-\mathsf{len}(K)} & (\mathsf{len}(K) < 8B) \\ K & (\mathsf{len}(K) = 8B) \\ H(K) \| 0^{8(B-L)} & (\mathsf{len}(K) > 8B) \end{cases}$$

であり，ipad は 1 バイトの 36 の B 回の繰り返し，opad は 1 バイトの 5c の B 回の繰り返しである．HMAC の構成を図 9.1 に示す．

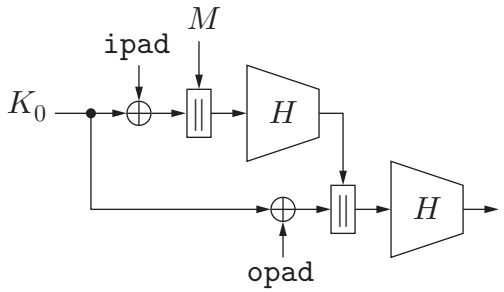


図 9.1: HMAC

9.2　安全性

HMAC の証明可能安全性は，Bellare, Canetti, Krawczyk [3] と Bellare [2] により論じられている．本節では後者の結果について記す．

$h : \Sigma^c \times \Sigma^b \to \Sigma^c$ を圧縮関数とする．なお，以下では $b \geq c$ を仮定する．$h^* : \Sigma^c \times (\Sigma^b)^+ \to \Sigma^c$ は，$s \in \Sigma^c$ と $M \in (\Sigma^b)^+$ について次のように定義される．$M = M_1 \| M_2 \| \cdots \| M_n \in (\Sigma^b)^+$ で，$1 \leq i \leq n$ について，$M_i \in \Sigma^b$ とし，

1. $s_0 = s$
2. $1 \leq i \leq n$ について，$s_i = h(s_{i-1}, M_i)$

とする．このとき，

$$h^*(s, M) = s_n$$

である．

h を用いて，GNMAC : $\Sigma^{2c} \times (\Sigma^b)^+ \to \Sigma^c$ を

$$\mathsf{GNMAC}(K_{\mathrm{out}} \| K_{\mathrm{in}}, M) = h(K_{\mathrm{out}}, h^*(K_{\mathrm{in}}, M) \| \mathtt{fpad})$$

と定義する．ここで，$\mathtt{fpad} \in \Sigma^{b-c}$ である．GNMAC の構造を図 9.2 に示す．

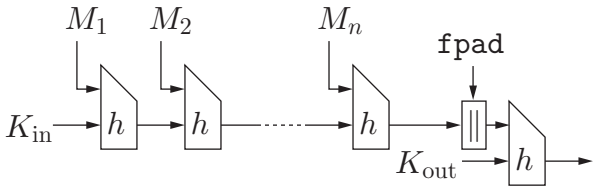


図 9.2: $\mathsf{GNMAC}(K_{\mathrm{out}} \| K_{\mathrm{in}}, M)$．$M = M_1 \| M_2 \| \cdots \| M_n \in (\Sigma^b)^n$ である．

次の定理は，$h : \Sigma^c \times \Sigma^b \to \Sigma^c$ が Σ^c を鍵空間とする擬似ランダム関数であれば，GNMAC も擬似ランダム関数であることを示している．

定理 9.1 (定理 3.4 [2]) A を GNMAC に対する prf 攻撃者とする．A の計算時間は t 以下，質問回数は $q\,(\geq 2)$ 以下とする．さらに，i 番目の質問のブロック数は m_i 以下であるとし，$n = \sum_{i=1}^{q} m_i$, $m = \max\{m_1, \ldots, m_q\}$ とする．このとき，h に対するある prf 攻撃者 A_1, A_2 が存在して

$$\mathrm{Adv}^{\mathrm{prf}}_{\mathsf{GNMAC}}(A) \leq \mathrm{Adv}^{\mathrm{prf}}_{h}(A_1) + (q-1)(n - q/2)\mathrm{Adv}^{\mathrm{prf}}_{h}(A_2) + \frac{q(q-1)}{2^{c+1}}$$

が成立する．ここで，A_1 の計算時間は t 以下，質問回数は q 以下であり，A_2 の計算時間は $O(mT_h)$ 以下，質問回数は 2 以下である．T_h は h の 1 回の計算に要する時間である．

次に，GHMAC-1 : $\Sigma^b \times (\Sigma^b)^+ \to \Sigma^c$ を

$$\mathsf{GHMAC\text{-}1}(K, M) = h^*(IV, (K \oplus \mathtt{opad}) \| h^*(IV, (K \oplus \mathtt{ipad}) \| M) \| \mathtt{fpad})$$

と定義する．GHMAC-1 の構造を図 9.3 に示す．また，$\overline{h} : \Sigma^b \times \Sigma^c \to \Sigma^c$ を，$\overline{h}(x, y) = h(y, x)$ と定義する．さらに，

$$K'_{\mathrm{out}} = h(IV, K \oplus \mathtt{opad}) = \overline{h}(K \oplus \mathtt{opad}, IV)$$
$$K'_{\mathrm{in}} = h(IV, K \oplus \mathtt{ipad}) = \overline{h}(K \oplus \mathtt{ipad}, IV)$$

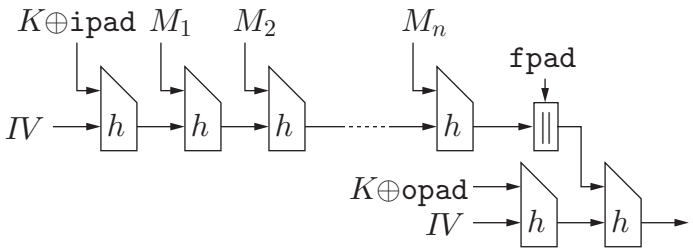


図 9.3: GHMAC-1

とする．このとき，

$$\begin{aligned}\mathsf{GHMAC\text{-}1}(K, M) &= h(K'_{\mathrm{out}}, h^*(K'_{\mathrm{in}}, M)\|\mathtt{fpad}) \\ &= \mathsf{GNMAC}(K'_{\mathrm{out}}\|K'_{\mathrm{in}}, M)\end{aligned}$$

が成立する．

次の補題は，$\overline{h}$ が Σ^b を鍵空間とする関連鍵攻撃のもとでの擬似ランダム関数であり，GNMAC が擬似ランダム関数であれば，GHMAC-1 が擬似ランダム関数であることを示している．

補題 9.2 (補題 5.2 [2]) $\Phi = \{\Delta_{\mathtt{opad}}, \Delta_{\mathtt{ipad}}\}$ とする．ここで，$\Delta_\alpha(K) = K \oplus \alpha$ である．A を GHMAC-1 に対する prf 攻撃者とする．A の計算時間は t 以下とする．このとき，$\overline{h}$ に対するある prf 攻撃者 A_1 が存在して

$$\mathrm{Adv}^{\mathrm{prf}}_{\mathsf{GHMAC\text{-}1}}(A) \le \mathrm{Adv}^{\text{rka-prf}}_{\overline{h},\Phi}(A_1) + \mathrm{Adv}^{\mathrm{prf}}_{\mathsf{GNMAC}}(A)$$

が成立する．ここで，A_1 の計算時間は t 以下，質問は $(\Delta_{\mathtt{opad}}, IV)$, $(\Delta_{\mathtt{ipad}}, IV)$ の 2 回である．

補題 9.2 では，$\overline{h}$ が関連鍵攻撃のもとで擬似ランダム関数であることが条件となっている．しかし，$\Phi = \{\Delta_{\mathtt{opad}}, \Delta_{\mathtt{ipad}}\}$ は，仕様で定められた定数によるものであり，攻撃者は選択できない．さらに，攻撃者の質問は，これも仕様で定められた IV に関する 2 回のみであり，この関連鍵攻撃は弱い攻撃とみなして差し支えないものと考えられる．

なお，GHMAC-1 の証明可能安全性の議論では，パディングに関する考察が省略されているが，パディングを考慮に入れた場合にも，同様の結果が導かれる．

9.3 まとめ

HMAC は，適応的選択文書攻撃に対する証明可能安全性を有しており，脆弱性の指摘されていない圧縮関数によるハッシュ関数を用いた場合，識別攻撃に要する圧縮関数の呼出し回数は $\Theta(2^{c/2})$ であると考えられる．なお，c は圧縮関数の出力長である．

SHA-1 を用いた HMAC に対する攻撃は，文献 [26, 33] で提案されているが，実用上の脅威は報告されていない．SHA-1, SHA-224/256/384/512 を用いた HMAC は安全なメッセージ認証コードと考えられる．

参考文献

[1] Ammar Alkassar, Alexander Geraldy, Birgit Pfitzmann, and Ahmad-Reza Sadeghi. Optimized self-synchronizing mode of operation. In Mitsuru Matsui, editor, *FSE*, volume 2355 of *Lecture Notes in Computer Science*, pages 78–91. Springer, 2001.

[2] Mihir Bellare. New proofs for NMAC and HMAC: Security without collision-resistance. In *CRYPTO 2006 Proceedings, Lecture Notes in Computer Science 4117*, pages 602–619, 2006. The full version is "Cryptology ePrint Archive: Report 2006/043" at `http://eprint.iacr.org/`.

[3] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In *CRYPTO '96 Proceedings, Lecture Notes in Computer Science 1109*, pages 1–15, 1996.

[4] Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th IEEE Symposium on Foundations of Computer Science*, pages 394–403, 1997.

[5] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining. In Yvo Desmedt, editor, *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 341–358. Springer, 1994.

[6] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences*, 61(3):362–399, 2000.

[7] Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Victor Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 527–545. Springer, 2005.

[8] Karl Brincat and Chris J. Mitchell. New CBC-MAC forgery attacks. In Vijay Varadharajan and Yi Mu, editors, *ACISP*, volume 2119 of *Lecture Notes in Computer Science*, pages 3–14. Springer, 2001.

[9] Morris Dworkin. Recommendation for block cipher modes of operation - methods and techniques. NIST Special Publication 800-38A, 2001.

[10] Morris Dworkin. Recommendation for block cipher modes of operation: The CCM mode for authentication and confidentiality. NIST Special Publication 800-38C, 2004.

[11] Morris Dworkin. Recommendation for block cipher modes of operation: The CMAC mode for authentication. NIST Special Publication 800-38B, 2005.

[12] Morris Dworkin. Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.

[13] Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard. Practical symmetric on-line encryption. In Johansson [20], pages 362–375.

[14] Pierre-Alain Fouque, Gwenaëlle Martinet, Frédéric Valette, and Sébastien Zimmer. On the security of the CCM encryption mode and of a slight variant. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *ACNS*, volume 5037 of *Lecture Notes in Computer Science*, pages 411–428, 2008.

[15] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[16] ISO/IEC 9797-1:1999. Information technology – security techniques – message authentication codes – part 1: Mechanisms using a block cipher, 1999.

[17] Tetsu Iwata and Kaoru Kurosawa. OMAC: One-key CBC MAC. In Johansson [20], pages 129–153.

[18] Tetsu Iwata and Kaoru Kurosawa. Stronger security bounds for OMAC, TMAC, and XCBC. In Thomas Johansson and Subhamoy Maitra, editors, *INDOCRYPT*, volume 2904 of *Lecture Notes in Computer Science*, pages 402–415. Springer, 2003.

[19] Keting Jia, Xiaoyun Wang, Zheng Yuan, and Guangwu Xu. Distinguishing and second-preimage attacks on CBC-like MACs. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *CANS*, volume 5888 of *Lecture Notes in Computer Science*, pages 349–361. Springer, 2009.

[20] Thomas Johansson, editor. *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*. Springer, 2003.

[21] Jakob Jonsson. On the security of CTR + CBC-MAC. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 76–93. Springer, 2002.

[22] Antoine Joux, Gwenaëlle Martinet, and Frédéric Valette. Blockwise-adaptive attackers: Revisiting the (in)security of some provably secure encryption models: CBC, GEM, IACBC. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 17–30. Springer, 2002.

[23] Antoine Joux, Guillaume Poupard, and Jacques Stern. New attacks against standardized MACs. In Johansson [20], pages 170–181.

[24] Jonathan Katz and Moti Yung. Complete characterization of security notions for probabilistic private-key encryption. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 245–254, 2000.

[25] Jonathan Katz and Moti Yung. Characterization of security notions for probabilistic private-key encryption. *Journal of Cryptology*, 19(1):67–95, 2006.

[26] Jongsung Kim, Alex Biryukov, Bart Preneel, and Seokhie Hong. On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1. In Roberto De Prisco and Moti Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 242–256. Springer, 2006.

[27] David A. McGrew and John Viega. The security and performance of the Galois/counter mode (GCM) of operation. In Anne Canteaut and Kapalee Viswanathan, editors, *INDOCRYPT*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer, 2004.

[28] David A. McGrew and John Viega. The security and performance of the Galois/counter mode of operation (full version). Cryptology ePrint Archive, Report 2004/193, 2004. `http://eprint.iacr.org/`.

[29] Silvio Micali, Charles Rackoff, and Bob Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal on Computing*, 17(2):412–426, 1988.

[30] Mridul Nandi. Improved security analysis for OMAC as a pseudorandom function. *Journal of Mathematical Cryptology*, 3(2):133–148, 2009.

[31] National Institute of Standards and Technology (NIST). The keyed-hash message authentication code (HMAC). Federal Information Processing Standards Publication 198-1, 2008.

[32] Erez Petrank and Charles Rackoff. CBC MAC for real-time data sources. *Journal of Cryptology*, 13(3):315–338, 2000.

[33] Christian Rechberger and Vincent Rijmen. New results on NMAC/HMAC when instantiated with popular hash functions. *The Journal of Universal Computer Science*, 14(3):347–376, 2008.

[34] Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, *ACM Conference on Computer and Communications Security*, pages 98–107. ACM, 2002.

[35] Phillip Rogaway. Nonce-based symmetric encryption. In *Proceedings of the 11th Fast Software Encryption Workshop (FSE 2004), Lecture Notes in Computer Science 3017*, pages 348–359, 2004.

[36] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In *ACM Conference on Computer and Communications Security*, pages 196–205, 2001.

[37] Doug Whiting, Russ Housley, and Niels Ferguson. Counter with CBC-MAC (CCM), AES mode of operation. Submission to NIST, 2002. `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf`.

[38] Kan Yasuda. The sum of CBC MACs is a secure PRF. In Josef Pieprzyk, editor, *CT-RSA*, volume 5985 of *Lecture Notes in Computer Science*, pages 366–381. Springer, 2010.