社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2004－SLDM－116 (22)
2004／10／22

組込みシステム向け IEEE 802.11i 暗号処理回路の実装

木村 基† 密山 幸男† 尾上 孝雄† 白川 功††

† 大阪大学大学院情報科学研究科情報システム工学専攻
†† 兵庫県立大学応用情報科学研究科

あらまし 本稿では，組込みシステム向け IEEE802.11i 暗号・復号処理回路の実装を行う．提案するアーキテクチャは，大きく分けて WEP/TKIP で用いられる RC4 処理部と AES-CCM 処理で用いられる AES 処理により構成される．少ない回路規模で要求性能を達成するため，RC4 処理部は，2 個のデータを結合しメモリアクセスを行うアーキテクチャを採用する．さらに AES 処理部は，CBC-MAC 処理と Counter-Mode 処理を重複させたパイプライン処理を採用する．提案する処理回路を VLSI 化した結果，ゲート数が約 18,000，消費電力は約 15mW となった．本回路は，60MHz 動作時に IEEE802.11a/g 規格の最大転送速度での暗号・復号処理が可能である．

キーワード 組込みシステム，IEEE802.11i，AES-CCM，TKIP，WEP

Embedded Implementation of IEEE802.11i Cipher Algorithms

Motoki KIMURA†, Yukio MITSUYAMA†, Takao ONOYE†, and Isao SHIRAKAWA††

† Department of Information Systems Engineering, Osaka University,
1-5 Yamada-Oka, Suita, Osaka, 565–0871 Japan
†† Graduate School of Applied Informatics, University of Hyogo,
1-3-3 HigashiKawasaki-Cho, Chuo-Ku, Kobe, 650–0044 Japan

Abstract This paper describes an embedded implementation of IEEE802.11i cipher algorithms for IEEE802.11a/g wireless communication systems. The proposed architecture consists mainly of the RC4 unit for WEP/TKIP and the AES unit for AES-CCM. The RC4 unit successfully adopts packed memory accessing architecture. As for the AES unit, overlapped pipeline scheme of CBC-MAC and Counter-Mode is exploited. The proposed cipher core has been implemented by using 0.18 *um* CMOS technology, which contains 18Kgates with dissipation of 15mW. This core also achieves the maximum transmission rate of IEEE802.11a/g, when operated at 60MHz clock rate.

Key words embedded system, IEEE802.11i, AES-CCM, TKIP, WEP

1. はじめに

近年，PDA，携帯電話などの携帯情報機器において，無線 LAN を利用したデータ通信が可能となりつつある中，そのセキュリティが問題視されている．そこで，無線 LAN IEEE802.11 MAC(Medium Access Control) [1] のセキュリティ拡張規格である IEEE802.11i [2] は，ユーザデータの高い秘匿性を持ち，IEEE802.11 パケット認証機能を提供する．IEEE802.11i では，WEP(Wired Equevalent Privacy), TKIP(Temporal Key Integrity Protocol) および AES-CCM(Advanced Encryption Standard in Counter-Mode with CBC-MAC)[3-5] を用いて暗号・復号処理を行うが，これらの方式は演算量が大きく，携帯情報機器での利用を考えた場合，組込みシステムのソフトウェアとして実装するだけでは十分な処理速度を達成するのは極めて困難である．加えて，これらの方式は 96 ビット，128 ビット単位の演算を多く含み，データパス幅に制限のある組込みプロセッサでの処理に適さない [6].

無線 LAN 規格 IEEE802.11b の標準暗号方式として用いられている WEP は，ソフトウェア実装が一般的であるが，無線 LAN 規格 IEEE 802.11a [7]/g [8] の要求性能を満たすことは難しい．さらに TKIP は，WEP に MIC(Message Integrity Code：メッセージ認証子) 生成機能と MAC フレーム認証機能を追加した方式であり，WEP 同様，ソフトウェア実装では要求性能を達成できない．

一方，AES-CCM は処理量が膨大であり，専用回路での実装が一般的である．これまで数多くの実装例 [9-12] が報告されているが，これらは処理性能が 500Mbps 以上，ゲート数が 25,000 ゲート以上であり，現状の無線 LAN の要求性能と比較して過剰な性能と回路規模を持つと言える [10].

このような背景から，本稿では無線 LAN 規格 IEEE802.11a/g の要求性能を満たし，かつ小面積で実装可能な IEEE802.11i 暗号・復号処理回路のアーキテクチャを提

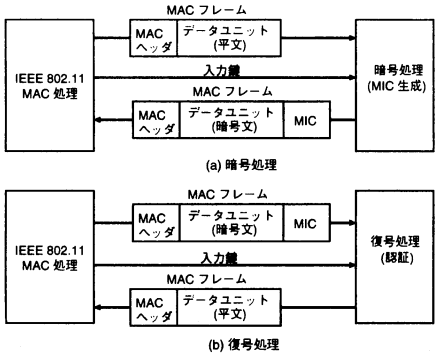


図 1 IEEE 802.11i 暗号・復号処理

案し，その実装を行う．本アーキテクチャは，WEP/TKIP で用いられる RC4 処理部，AES-CCM で用いられる AES 処理部などにより構成される．少ない回路規模で要求性能を達成するため，RC4 処理部は，2 個のデータを結合しメモリアクセスを行うアーキテクチャを採用する．さらに AES 処理部は，CBC-MAC と Counter-Mode の 2 種類の AES 処理を重複させたパイプライン処理を採用する．

2. IEEE 802.11i 暗号アルゴリズム

2.1 IEEE 802.11i 暗号・復号処理の概要

IEEE 802.11i における暗号・復号処理の動作を図 1 に示す．暗号処理では，まず，MAC 処理部から入力鍵と MAC フレームを受け取り，初期化処理，MAC ヘッダ解析処理を行う．次に，フレーム内データユニットに含まれる平文の暗号処理，MIC の生成処理を行った後，MAC フレームを再構成し出力する．

一方，復号処理では，フレーム内データユニットに含まれる暗号文の復号処理を行うとともに，入力される MIC と内部で生成した MIC との比較による MAC フレームの認証処理を行う．

2.2 WEP/TKIP 処理

WEP/TKIP 暗号方式の概略を図 2 に示す．WEP/TKIP 暗号方式は，鍵生成処理と共通鍵暗号 RC4 で構成される．WEP 方式では，MAC ヘッダから得られる IV (Initialization Vector : 初期化ベクトル) と入力鍵とを結合してできる 64 ビットの RC4 鍵を生成する．一方 TKIP 方式では，MAC アドレス，IV を用いて入力鍵を撹拌することにより 128 ビットの RC4 鍵を生成する．

RC4 処理では MAC フレームが入力されるたびに，まず，シャッフリング処理を行う．シャッフリング処理では，RC4 鍵を用いて 256 バイトの初期擬似乱数を生成する．この初期疑似乱数に対し，さらに追加置換処理と呼ばれる 1 バイトデータ単位の置換処理を施すことにより，疑似乱数を生成する．最後に，生成した擬似乱数と平文，または暗号文との排他的論理和を求め，暗号文，平文をそれぞれ出力する．

2.3 AES-CCM 処理

AES-CCM 暗号方式の概略を図 3 に示す．AES は NIST(National Institute of Standards and Technology) が 2000 年に標準化した，Rijndael [4] アルゴリズムに基づくブロック暗号である．

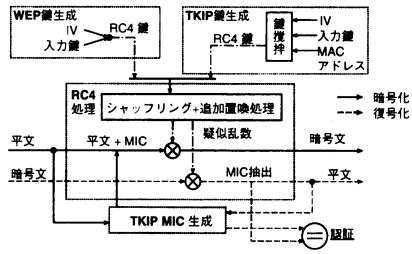


図 2 WEP/TKIP 暗号方式

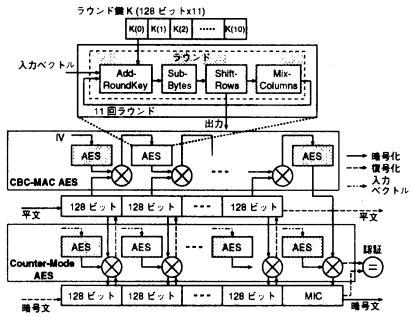


図 3 AES-CCM 暗号方式

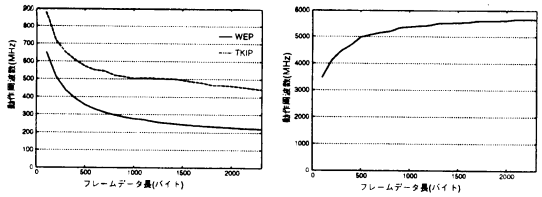
AES-CCM 方式では，128 ビットの入力データに対して，128 ビットの入力鍵を用い，Counter-Mode AES を用いた暗号・復号処理，CBC-MAC AES を用いた MAC フレーム認証処理を行う．Counter-Mode AES では，カウンタを用いて生成した 128 ビットの入力ベクトルに AES 処理を施す．次に処理結果と入力する平文，または暗号文との排他的論理和を求め，暗号文，平文をそれぞれ出力する．CBC-MAC AES では，生成した IV に AES 処理を施す．次に，処理結果と平文との排他的論理和を求め，その処理結果を次段の AES 処理の入力とする．この処理を繰り返すことにより MIC を生成し，MAC フレーム認証処理を行う．

AES 処理では，まず，MAC フレームごとに与えられる 128 ビットの初期鍵に対して鍵スケジューリング処理を行うことで，128 ビットのラウンド鍵 K を 11 個生成する (図 3 $K(i)$)．AES のラウンド処理は，4 つの基本演算 AddRoundKey, SubBytes, ShiftRows および MixColumns から構成される．また，このラウンド処理は 11 回繰り返され，先に生成した 11 個のラウンド鍵が 1 ラウンドごとに順に用いられる．AES 暗号・復号処理の中間結果はステートと呼ばれる 4×4 バイトの行列として扱われる．

各基本演算の内容は次の通りである [3]．AddRoundKey はラウンド鍵とステートの排他的論理和を求める．SubBytes はステートの各バイトに対して S-Box と呼ばれる置換テーブルを用い，非線形置換処理を行う．ShiftRow はステートの各行に対して異なるバイト数だけ巡回シフトする．MixColumns はステートの各列 4 バイトに対し行列演算を施す．

2.4 演算量解析

暗号処理回路のアーキテクチャを決定するため，組込みシステムに広く用いられている ARM9 プロセッサの命令セットシミュレータ ARMulator を用いて演算量解析を行った．MAC



(a)WEP/TKIP (b)AES-CCM

図 4 IEEE802.11a/g の最大転送速度を達成するのに必要な動作周波数

表 1 WEP 処理の演算量

フレームデータ長	演算量 (Mcycles/sec)			必要動作周波数 (MHz)
	シャッフリング	追加置換	その他	
100	583	54.1	13.5	651
500	218	109	27.4	354
1000	126	120	30.0	276
2000	68.4	126	32.4	227

フレームのデータ長を 100 バイトから 2,300 バイトまで変化させた場合に，IEEE802.11a/g の最大転送速度を達成するのに必要な動作周波数を図 4 に示す．

解析結果から，IEEE802.11a/g の最大転送速度での暗号・復号処理に必要となる周波数は，どのデータ長の場合でも，WEP，TKIP，AES-CCM でそれぞれ，220MHz，440MHz，3.5GHz 以上となる．現状の ARM9 プロセッサの最大動作周波数が 250MHz であることを鑑みると，ソフトウェア実装で IEEE802.11a/g の要求性能を満たすことが極めて困難であることがわかる．

特に，AES-CCM，TKIP については 96 ビット，128 ビット単位の演算を多く含むため，データパス幅に制限のある組込みプロセッサでは，並列処理などによる処理の効率化も多くは望めない．

また，WEP/TKIP については，データユニット長が短い場合，暗号・復号処理に必要な動作周波数が増加することがわかる．これは，表 1 に示すように，MAC フレーム入力毎に実行されるシャッフリング処理が暗号処理全体のサイクル数の大部分を占めるためである．

以上の解析結果に基づき，提案する IEEE802.11i 暗号処理回路のアーキテクチャを以下に述べる．

3. 暗号・復号処理回路の設計

3.1 全体構成

提案する暗号・復号処理回路のアーキテクチャを図 5 に示す．本回路は，動作モードの選択により単一の回路で暗号あるいは復号処理を実行するものであり，RC4 処理部，鍵攪拌部，MIC/CRC 生成部，ヘッダ解析部，AES 処理部および 128 ビットの鍵レジスタ，出力レジスタにより構成される．暗号処理と復号処理の基本構成は同じであるが，暗号処理では，暗号文と MIC の出力を行い，復号処理では，暗号文を復号処理してから MIC を生成し MAC フレーム認証処理を行うという点で異なる．提案する処理回路は 8 ビットの入出力ポートを持ち，フレーム内データを 8 ビット単位で順次処理する．

内部処理は大きく初期化処理と暗号・復号処理に分かれる．初期化処理は，WEP/TKIP の場合，鍵攪拌処理およびシャッフリング処理，AES-CCM の場合，鍵スケジューリング処理およびヘッダ解析処理から構成され，MAC ヘッダの入力が完了するまでに実行される．

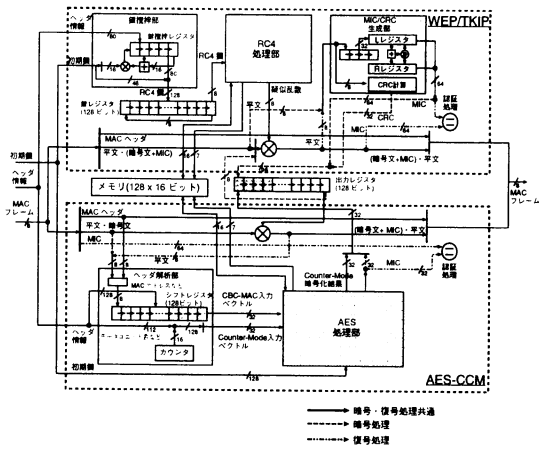


図 5 暗号・復号処理回路構成

ヘッダ解析部では，ヘッダ情報，8 ビット単位で入力される MAC ヘッダ，平文 (復号処理時は暗号文から得られる平文) から，シフトレジスタを用いて，128 ビットの CBC-MAC 入力ベクトルを生成する．Counter-Mode 入力ベクトルは，ヘッダ情報とカウンタの値を用いて生成する．また，3.3 節で述べるように，AES 処理部では 32 ビットデータパス構成を採用するため，ヘッダ解析部は 32 ビット単位で入力ベクトルを出力する．

鍵攪拌部では，TKIP で処理する場合に初期鍵およびヘッダ情報をもとに鍵攪拌処理を行う．鍵攪拌処理は，16 ビット単位の加算処理，巡回シフト処理，排他的論理和を求める処理を組み合わせた処理を 25 回繰り返すものである．本回路では，16 ビット加算器と 80 ビットのシフトレジスタをそれぞれ 1 個用いて鍵攪拌処理部を構成し，25 サイクルで 128 ビットの RC4 鍵を生成して鍵レジスタに書き込む．WEP の場合は鍵攪拌処理は行わず，ヘッダ情報から抽出した IV を入力鍵と結合し，64 ビットの RC4 鍵を生成して鍵レジスタに書き込む．

MIC/CRC 生成部では，TKIP の場合は MIC および CRC を，WEP の場合は CRC を生成する．MIC 生成処理では，まず，シフトレジスタを用いて 8 ビットの平文入力を 32 ビットデータに変換し，L レジスタに出力する．次に，L, R レジスタ内のデータ加算・シフト処理を行う．この処理を MAC フレームの平文データが全て入力されるまで繰り返した後，L, R レジスタの値を結合し 64 ビット MIC を出力する．

本回路では，フレーム内データを 8 ビット単位で出力するが，AES Counter-Mode 暗号処理結果は 32 ビット単位で，MIC，CRC はそれぞれ 64 ビット単位，32 ビット単位で出力する．そのため，暗号処理結果，MIC，CRC を出力レジスタを用いて 8 ビット単位の出力に変換する．

3.2 RC4 処理部アーキテクチャ

2.2 節で述べたように，RC4 処理は RC4 鍵に対してシャッフリング処理と追加置換処理を行うことで疑似乱数を生成する．RC4 処理はワード幅 8 ビットのメモリアクセスの制御，およ

```
procedure shuffling
   k(0 : L − 1) : 8bit; RC4 key;
   a(0 : 255),r1,r2,c : 8bit;
begin
1  for i = 0 until 255 do
2     a(i) = i;                                   — (1)
3  c = 0;
4  for i = 0 until 255 do
5     r1 = a(i);                                  — (2)
6     c = {c + r1 + k(i%L)} % 256;
7     r2 = a(c);                                  — (3)
8     a(c) = r1;
9     a(i) = r2;                                  — (4)
end
```

図 6　シャッフリング処理

びアドレス生成を行う単純なハードウェアで実現できる．ところが，2.4 節で述べたように，MAC フレームのデータ長が短い場合，シャッフリング処理の全体処理に占める割合が大きくなる．したがって，RC4 処理部のアーキテクチャ設計においては，シャッフリング処理の効率化を図る必要がある．

シャッフリング処理を図 6 に示す．シャッフリング処理では，生成される疑似乱数を格納しておくために 256 × 8 ビットのメモリが必要となる．このメモリ領域を要素数 256 の配列 $a(n)\{n = 0, ..., 255\}$ とする．また，入力される RC4 鍵を 8 ビットずつ分け，配列 $k(n)\{n = 0, ..., L-1\}$ とする．L の値は，64 ビットの RC4 鍵を用いる WEP の場合 8 であり，128 ビットの RC4 鍵を用いる TKIP の場合 16 である．

専用回路を用いてシャッフリング処理を実装する場合，処理の大半を占めている置換処理によるメモリアクセスを削減することが重要となる．削減方法としては，メモリアクセスの並列化が考えられる．しかしながら，図 6 に示すように，シャッフリング処理においては，$a(i)$ および $a(c)$ の値の間にデータの依存関係が存在するため，メモリアクセスを並列化することはできない．そこで，本研究では，128 × 16 ビットのメモリを用い，2 個の 8 ビットデータを結合し 1 個のデータとしてメモリアクセスを行う手法を提案する．(図 7)．

提案手法では，図 6 の i, $(i+1)$ 番目 $(i = 2j;\ 0 \leqq j \leqq 127)$ の 2 個の置換処理 (5〜9 行目) を，図 7 の j 番目の繰り返し (5〜12 行目) でまとめて実行する．このうち，図 7(3), 7(4) は，それぞれ図 6 の i, $(i+1)$ 番目の置換処理の (3) の部分に対応する．また，図 7(2), 7(5) では，それぞれ図 6(2), 6(4) の処理を実行する．

ただし，図 7 についても，図 6 と同様に，シャッフリング処理の中間データ $a(j)$ と $a(c/2)$ の間には，依存関係が存在する (e.g. $j = 0$, $k(0) = 1$)．その場合，$(2*j)$, $(2*j+1)$, c の値から依存関係を判定し，メモリアクセス順序の入れ替わりによるデータの上書きを防ぐ制御を行う．

本手法を用いた場合，配列初期化処理に要するアクセス回数は 8 ビット処理の場合の半分となる (図 7(1))．また，図 7(2), 7(5) では 2 個のデータに同時にアクセスするため，置換処理 2 回につき，2 回のメモリアクセスを削減できる．

図 6 の方法を用いて 8 ビット処理を行う回路と，提案法を用いて 2, 4 個の 8 ビットデータを結合し 16, 32 ビット処理を行う回路について，シャッフリング処理におけるメモリアクセス回数の比較を表 2 に示す．32 ビット処理回路は，16 ビット処理回路と比較して，メモリバス幅は 2 倍となるが，図 7(2),7(5) 以外で複数の 8 ビットデータへの同時アクセスはできないため，アクセス回数は約 20% しか削減されない．加えて，32 ビット処理回路においては，16 ビット処理回路と比較し，データ依存関係が複雑になり，回路規模が増加する．以上のことを考慮し，本研究では 16 ビット処理回路を採用する．16 ビット処理により 8 ビット処理と比較し約 300 ゲートの回路規模の増加でシャッフリング処理におけるメモリアクセス回数を約 30 % 削減することができる．

```
define {r2, r1}_j
   if j = 0 then r2||r1;
   else r1||r2;

procedure shuffling16
   k(0 : L − 1) : 8bit; RC4 key;
   a(0 : 127) : 16bit;
   r11,r12,r21,r22,c,tmp : 8bit;
begin
1  for j = 0 until 127 do
2     a(j) = {(2 * j + 1), (2 * j)}_0;            — (1)
3  c = 0;
4  for j = 0 until 127 do
5     {r21, r11}_0 = a(j);                        — (2)
6     c = {c + r11 + k((2 * j)%L)} % 256;
7     {tmp, r12}_{c%2} = a(c/2);                  — (3)
8     a(c/2) = {tmp, r11}_{c%2};
9     c = {c + r21 + k((2 * j + 1)%L)} % 256;
10    {tmp, r22}_{c%2} = a(c/2);                  — (4)
11    a(c/2) = {tmp, r21}_{c%2};
12    a(j) = {r22, r12}_0;                        — (5)
end
```

図 7　提案シャッフリング処理

表 2　シャッフリング処理におけるメモリアクセス回数

8 ビット処理	16 ビット処理	32 ビット処理
1,282	896	704

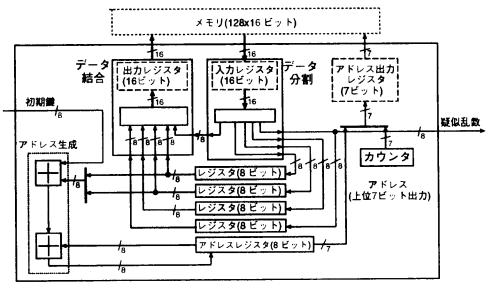


図 8　RC4 処理部

提案する RC4 処理部の回路構成を図 8 に示す．本回路では，RC4 処理における 8 ビットデータ処理をワード幅が 16 ビットのシングルポートメモリを用いて行う．データ分割部は，16 ビットデータをメモリから読み出し，2 個の 8 ビットデータに分割しレジスタに保存する．一方データ結合部は，4 個のレジスタおよび，データ分割部の出力から 2 個の 8 ビットデータを結合し，16 ビットデータとしてメモリに書き込む．

アドレス生成部では，2 つのレジスタ内データから 1 つを選び鍵データと加算した後，8 ビットのアドレスレジスタ内データを更に加算しアドレスレジスタに書き戻す処理を行う．

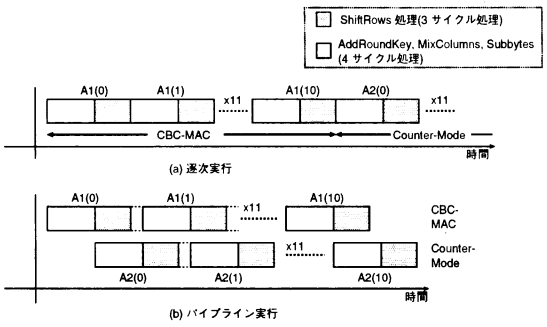


図 9 AES 暗号処理タイミング図

3.3 AES 処理部アーキテクチャ

2.3 節で述べたように，AES 処理は，基本演算 AddRoundKey, SubBytes, ShiftRows および MixColumns からなるラウンド処理を 11 回繰り返すことにより行われる．このうち，AddRoundKey, MixColumns は 32 ビット単位で実行され，SubBytes は 8 ビット単位で実行される．また，ShiftRows では，128 ビットデータをステートと呼ばれる 4×4 バイトの行列とし，各行につき異なるバイト数巡回シフトを行う．

AddRoundKey, MixColumns の処理単位に基づき AES 処理回路を 32, 64, 128 ビットデータパスで構成した場合，AES 1 ラウンドあたりの処理サイクル数はそれぞれ 4, 2, 1 サイクルと見積もられる．すなわち，128 ビットデータの処理に必要なサイクル数は，それぞれ 88, 44, 22 サイクルとなり，どの構成を採用しても，40MHz 以下の動作周波数で IEEE802.11a/g 規格の要求性能を満足できることがわかる．

本研究では回路規模を考慮し，AES 処理回路を 32 ビットデータパスで構成する．さらに，ShiftRows 処理に含まれる 2, 3 バイトの巡回シフト処理を 1 バイト・シフタを用いて，それぞれ 2, 3 サイクルで処理する．

この場合，CBC-MAC/Counter-Mode AES を 1 ラウンド処理するのに必要なサイクル数は，ShiftRows 演算に 3 サイクル，ShiftRows 以外の基本演算に 4 サイクル，合計 7 サイクルとなる (図 9(a))．

ここで，AES-CCM 暗号方式では，CBC-MAC AES と Counter-Mode AES の 2 種類を実行するため，本研究では，これらの処理を重複させたパイプライン処理を採用することにより，ShiftRows 処理におけるレイテンシを隠蔽する (図 9(b))．

AES 処理部の回路構成を図 10 に示す．本回路は 32 ビットのシフトレジスタ 4 個から構成される CBC-MAC レジスタと Counter-Mode レジスタを持ち，MAC ヘッダ解析を除く AES-CCM 処理を実行する．128 ビットデータは，図 10 中の列インデックス [0]～[3] に最下位ビットから順に 32 ビット単位で格納される．

AES 処理を行う場合，まず入力ベクトルをレジスタに格納する．その後，CBC-MAC レジスタより 32 ビットデータを順次読み出し，MixColumns, AddRoundKey, SubBytes 演算を実行し，再び CBC-MAC レジスタに結果を格納する．次に，CBC-MAC レジスタ内部で ShiftRows 演算を実行する．これと並行して，Counter-Mode について，MixColumns, AddRoundKey, SubBytes 演算を実行する．

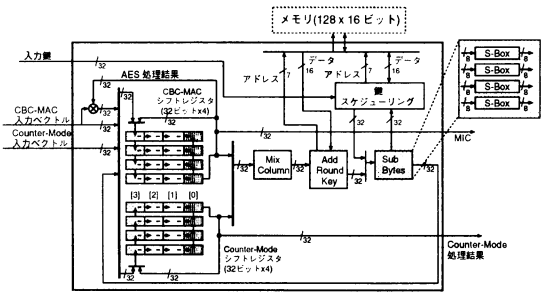


図 10 AES 処理部

以上の処理を CBC-MAC, Counter-Mode について交互に繰り返すことで，CBC-MAC, Counter-Mode レジスタに AES 処理結果が格納される．Counter-Mode AES 処理結果は，次の Counter-Mode 入力ベクトルを受け取ると同時に出力する．これに対して，CBC-MAC AES では，32 ビット単位で次の入力ベクトルと AES 処理結果の排他的論理和を求め，再度 AES 処理を行う．この操作を繰り返し，MAC フレームの最後の AES 処理終了後，CBC-MAC レジスタから MIC を出力する．

SubBytes 部は，S-Box 演算器 4 個で構成される．S-Box 演算は，アファイン変換の後にガロア体 $GF(2^8)$ 上での逆元演算を行うものであり，256×8 ビットのテーブルを用いて実装することができる．本研究では回路規模削減のため，文献 [13] で提案されている合成体 $GF(((2^2)^2)^2)$ を用いた手法で実装する．

ここで，図 9(a) に基づき実装する場合，図 10 のうち，CBC-MAC レジスタと Counter-Mode レジスタのうち 1 個が不要となるが，代わりに CBC-MAC AES 処理結果を保持する 128 ビットのレジスタが必要となる．よって，図 9(a), (b) のどちらの方式で実装しても回路規模は大きく変化しない．以上より，本回路は図 9(b) のパイプライン処理を採用することで，制御回路の増加のみで ShiftRows 処理のレイテンシを隠蔽し，処理速度の向上することが可能となる．

3.4 メモリ共有化

WEP/TKIP 処理と AES-CCM 処理では，拡張鍵を保持するためそれぞれ 2,048 ビット，合計 4,096 ビットのメモリが必要となる．本回路では，IEEE 802.11i 暗号処理において，各暗号方式が選択的に用いられることを利用し，図 5 に示すように，WEP/TKIP 処理と AES-CCM 処理で 128×16 ビットのシングルポートメモリを共有することにより，メモリサイズを削減する．

4. 実装結果

提案する暗号・復号処理回路を VHDL を用いて記述し，Synopsys Design Compiler により日立製作所 0.18 μm CMOS テクノロジで VLSI 化を行ったところ，ゲート数が 17,832，最大動作周波数が 72MHz，メモリサイズが 2,048 ビットとなった．表 3 に実装結果を示す．本処理回路のうち，AES-CCM 処理部のゲート数は約 9,800 であり，既存の AES-CCM 処理回路 [10] と比較して回路規模を約 61% 削減している．

MAC フレームのデータ長を 10 バイトから 2,300 バイトまで変化させた場合に，本処理回路を用いて IEEE802.11a/g の最大転送速度を達成するのに必要な周波数を図 11 に示す．本

表 3　暗号・復号処理回路諸元

ゲート数	AES-CCM 処理	9,752
	WEP/TKIP 処理	4,834
	全体制御	3,446
	処理回路全体	17,832
メモリサイズ		2 Kbit
最大動作周波数		72MHz

日立製作所 0.18μm CMOS テクノロジ

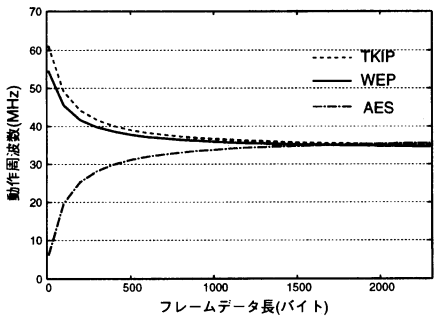


図 11　提案処理回路で IEEE802.11a/g の最大転送速度を達成するのに必要な動作周波数

処理回路は，いかなるフレームデータ長に対しても 60MHz 動作時に IEEE802.11a/g の最大要求性能での暗号・復号処理が可能である．

論理合成後の回路にゲートレベルシミュレーション結果をバックアノテートしたものを用いて，Synopsys DesignPower により，各暗号方式における消費電力を見積もった．図 11 より，WEP, TKIP, AES-CCM において IEEE802.11a/g の要求性能を達成するために必要な動作周波数は，それぞれ 55MHz, 60MHz, 36MHz であることから，WEP, TKIP, AES-CCM での消費電力は，それぞれ 17.5mW, 19.8 mW, 12.3 mW となった (表 4)．

ここで，クロックの供給による消費電力を求めたところ，それぞれ 11.4mW, 12.5mW, 7.5mW となった．これは，TKIP, AES-CCM 方式で用いる 128 ビット，96 ビット単位の中間結果を保持するためのレジスタを多く搭載しているためであると考えられる．

そこで，Gated Clock を導入し，選択される暗号方式で利用しないモジュールへのクロックの供給を停止することで，消費電力の削減を図った．図 5 のうち，WEP 動作時には，RC4 処理部および MIC/CRC 生成部に，TKIP 動作時は，鍵撹拌部，RC4 処理部および MIC/CRC 生成部に，AES-CCM 動作時には，ヘッダ解析部および AES 処理部にそれぞれクロックを供給するものとした．

Gated Clock の有無による WEP, TKIP, AES-CCM 処理時の消費電力の比較を表 4 にまとめる．これにより Gated Clock を導入することで，WEP,TKIP, AES-CCM 処理時にそれぞれ消費電力を約 28%, 27%, 20% 削減可能と見積もられた．

以上より，本処理回路は小面積化，低消費電力化を実現しており，回路規模，消費電力の大幅な増加なしに，IEEE802.11 MAC 処理部 [14] [15] と共に集積することで，組込みシステムでの利用が可能となる．

表 4　暗号処理回路の消費電力 (電源電圧 1.6V)

	WEP (55MHz 動作)	TKIP (60MHz 動作)	AES-CCM (36MHz 動作)
Gated Clock なし	17.5mW	19.8 mW	12.3 mW
Gated Clock あり	12.7mW	14.5 mW	9.9 mW

5. 結　　論

本稿では，組込みシステム向け IEEE802.11i 暗号・復号処理回路のアーキテクチャを提案し，その実装を行った．少ない回路規模で IEEE802.11a/g の要求性能を満たすため，RC4 処理部では，2 個の 8 ビットデータを結合しメモリアクセスを行うことで，シャッフリング処理の効率化を行った．さらに AES 処理部では，CBC-MAC AES と Counter-Mode AES の重複パイプライン処理を採用した．提案する処理回路は，ゲート数が約 18,000，消費電力が約 15mW となり，IEEE802.11 MAC 処理部と共に集積することにより，組込みシステムでの利用が可能となった．また，60MHz 動作時に IEEE802.11a/g 規格の最大転送速度での暗号・復号処理を実現した．

文　　献

[1] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," IEEE Std 802.11, 1999.

[2] "Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications, Specification for Enhanced Security," IEEE 802.11i-D7.0, 2003.

[3] National Institute of Standards and Technology (NIST): "Advanced Encryption Standard(AES), FIPS Publication 197," 2001.

[4] J. Daemen and V. Rijmen: "AES Proposal, Rijndael," 1999.

[5] D. Whiting, R. Housley, and N. Ferguson: "IEEE P802.11 Wireless LANs, AES Encryption & Authentication Using CTR Mode & CBC-MAC," IEEE Tech. Rep. IEEE 802.11-00/362, Oct. 2000.

[6] T. J. Wollinger, M. Wang, J. Guajardo, and C. Paar: "How well are high-end DSPs suited for the AES algorithms?," The Third AES Candidate Conference, pp. 94–105, Apr. 2000.

[7] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications," IEEE Standard 802.11a, 1999.

[8] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications, Further Higher Data Rate Extension in the 2.4GHz Band," IEEE Standard 802.11g, 2003.

[9] SiWorks, SCAES-CCM Product Brief

[10] Helion Technology, AES for IEEE802.11i

[11] NTRU, NTRU Aerolink, AES Hardware Cores

[12] K. Vu and D. Zier: "FPGA Implementation AES for CCM Mode Encryption Using Xilinx Spartan-II," ECE 679, Advanced Cryptography, Oregon State University, 2003.

[13] A. Satoh, S. Morioka, K. Takano, and S. Munetoh: "A Compact Rijndael Hardware Architecture with S-Box Optimization," in Proc. of 7th International Conference on the Theory and Application of Cryptology and Information Security(ASIACRYPT), LNCS Vol.2248, pp.239–254, Dec. 2001.

[14] J. Thomson, et al.:"An Integrated 802.11a Baseband and MAC Processor," ISSCC Digest of Technical Papers, pp.126–127, Feb. 2002.

[15] M. Iliopoulos, A. Maniatopoulos and T. Antonakopoulos, "Design and Implementation of a MAC Controller for the IEEE802.11 Wireless LAN," International Journal of Electronics, Tailor&Grancis Vol.88, No.3, pp.271-285, 2001.