DVD暗号LSIの開発

Development of cipher LSI for DVD

山口 聡，吉田 成孝，鈴木 敏雄

Satoshi Yamaguchi, Shigetaka Yoshida, Toshio Suzuki,

佐々木 努，河原 哲也，遠藤 秀人

Tsutomu Sasaki, Tetsuya Kawahara, Hideto Endo

要　旨　DVD録画機で著作権を保護しつつ商用コンテンツの記録を可能とするため，記録型DVDで採用されているコンテンツ暗号化方式"Content Protection for Recordable Media"(CPRM)に準拠した暗号化，復号化を行なうLSI(CPRM LSI)の開発を行なった。暗号に関わる処理をLSI内部で完結させることで，機密情報の保護とLSI制御の容易化を実現し，独立した暗号化処理系と復号化処理系を備えることにより，録再同時動作への対応を可能とした。

Summary　We have developed a dedicated CPRM LSI that is constructed with the encryption and the decryption blocks that are compliant with the "Content Protection for Recordable Media (CPRM) Specification Introduction and Common Cryptographic Elements rev. 0.94" and the "CPRM Specification DVD Book rev. 0.95". The CPRM technology is used for recording commercial content by a DVD recorder while protecting copyright of such content. Since all enciphering related processing is accomplished in this LSI, it makes the protection of the secret information stable and the control of the LSI easier. The LSI has the encryption and the decryption system implemented independently, so that it can provide the simultaneous operation of recording and playback to user.

キーワード：DVD，CPRM，暗号，LSI

1. まえがき

近年，アナログVTRを代替するデジタル録画機器が注目される中，DVD録画機の需要も拡大している。これは，機器，メディアの低価格化とともに，ランダムアクセス，デジタル記録などDVDメディアならではの特徴が消費者に受け入れられつつあることを示すものである。デジタル記録機器は，ユーザーに対して利便性をもたらす一方，デジタル化されたコンテンツは複製による劣化がないため，コンテンツの著作権を所有する者にとっては著作権侵害の脅威となり得る。こうした著作権者の懸念を払拭し，魅力あるコンテンツの潤沢な供給を促すため，デジタル記録機器には著作権を保護，管理する仕組みが必要とされる。DVD録画機では，コンテンツに付加される複製制御情報に従い，商用コ

ンテンツを暗号化して記録することで,コンテンツの複製を制御している。今回開発したLSI(CPRM LSI)は,記録型DVDのコンテンツ暗号化方式であるCPRMに準拠した暗号化，復号化の機能を提供するものである。

2.CPRM LSIの概要

CPRM LSIの主たる機能は記録ストリームの暗号化と再生ストリームの復号化である。暗号化においては,暗号化されていないストリームデータを入力とし，ストリームのpackを解析して，その結果をもとに画像，音声情報を含むpack(AV pack)に対して暗号化を施し，暗号化ストリームデータとして出力する。復号化においては,暗号化されているストリームデータを入力とし，ストリームのpackを解析して，その結果をもとにAV packに対して復号化を施し,暗号化されていないストリームデータに復元して出力する。また，暗号化，復号化の際に必要となる各種の鍵の生成，管理もCPRM LSIが担う。

3.CPRM LSIの特徴

LSIの設計に際し，機密情報の保護とCPUの負荷低減を基本的な方針とした。表1には主な仕様を,図1にはCPRM LSIのブロックでを示す。

3.1 構造

3.1.1 ストリーム処理

CPRM LSIはストリームデータを処理するパスを2系統持っている。一方は記録ストリームデータを暗号化し,他方は再生ストリームデー

表1 CPRM LSI 仕様

プロセス	0.35μm CMOSゲートアレイ相当
回路規模	19万ゲート
電源電圧	3.3V
動作温度	-40 ～ 125℃
クロック周波数	27MHz
データ転送レート	5Mbyte/sec以上
データ出力遅延時間	12μsec以下

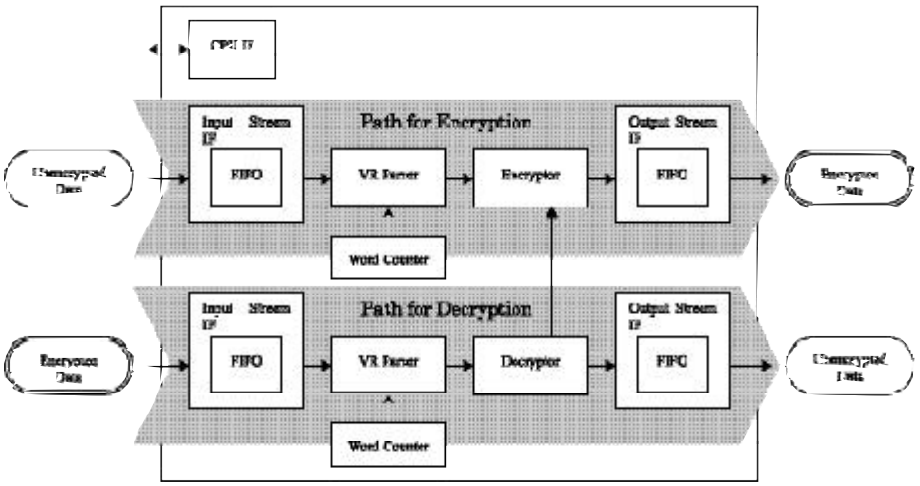


図1 CPRM LSIブロック

タの復号を行なう。録再同時動作を実現するために，これら2系統のパスは独立して動作が可能となっている。暗号化，復号化は64ビットのデータを単位とする処理であるため，各ストリームパスの入出力段にFIFOを配置することでLSI外部とのデータ転送が間欠化することを抑制している。また，本LSIでは，VR Parserを内蔵することで，ストリームデータのpackを解析し，暗号化，復号化時に必要となる情報を自動的に取得している。このため，ストリームデータの転送動作に関して，本LSIをFIFOと等価とみなすことができ，CPUに多大な負荷のかかる記録，再生時に，CPRM LSIの制御に関わる処理は最小限となっている。

3.1.2 鍵生成

MKBはディスクに予め記録されているデータで，メディア鍵の生成に用いられる。MKBを処理する作業は，判断，分岐を伴う複雑なものである。MKBの処理はまた，実行頻度も低く，処理速度も要求されないため，修正が比較的容易なソフトウェアによる実装が製造の観点から考えると妥当である。しかしながら，本LSIでは，機密情報を保護するため，MKB処理をハードウェアで実装することを選択した。MKBがディスクに記録されているデータであるため，MKBの入力ポートを再生ストリーム入力と共用とした。入力されたMKBはDecryptorで処理される。Decryptorは，MKBからメディア鍵を算出し，さらに，複数の工程を経てタイトル鍵を生成する。このタイトル鍵を使用して，Encryptor，Decryptorは，暗号化，復号化に使用するコンテンツ鍵を生成する。Encryptorは，Decryptorのサブセットで，DecryptorからMKB処理とその他鍵生成を行なうモジュールを省いた構成となっている。

3.2 開発手法

本LSIの開発では言語記述による回路設計手法を用いた。言語で記述されたデザインは，回路図入力に比べ，可読性，移植性に優れる。一方，言語記述では，論理合成を行なわなければ実際の回路が確定しないため，回路設計時点での速度性能の予測精度は低くなる。本LSIでは，処理速度を要求される回路ブロックを先行して設計し，論理合成とその結果に基づく設計及び論理合成条件の修正を繰り返すことで，速度性能の予測を行なった。

本LSIでは，機密情報を保護するため，内部ノードのモニター出力を最小限にとどめている。単純にモニター出力を制限すると，LSIの機能シミュレーション，動作検証が困難となってしまう。機能シミュレーションを十分なものとするため，必要なモニター出力を備えるが，それらを容易にマスクできるような構成で本LSIを設計した。シミュレーションの工程が終了した後，配線修正にてこれらモニター出力をマスクしているので，製品となったLSIから機密情報が漏洩することはない。また，LSIの設計と隔離された環境でソフトウェアモデルを構築し，LSIとソフトウェア双方の動作を比較，検証することで，規格への準拠を確実なものとした。

4. CPRM LSIの詳細

4.1 CPU IF

アドレスバス，データバスを持ち，RD，WR，CSによってリード/ライトを行う。また，各種割り込み出力としてIRQ出力端子を備えている。

4.2 Input Stream IF

Input Stream IFはストリーム入力を行う部分であり，暗号化処理系，復号化処理系それぞれにインターフェースを備える。データの制御はREQ，ACKで行い，これらの信号の極性はレジスタ設定により変更することが可能である。16ビット×16ワードのFIFOを備えている。また，復号化処理系の入力インターフェースはストリームデータの他，MKBデータ入力にも使用する。

4.3 Output Stream IF

Output Stream IFはストリーム出力を行う部分であり，暗号化処理系，復号化処理系それ

ぞれにインターフェースを備える。データの制御はREQ，ACKで行い，これらの信号の極性はレジスタ設定により変更することが可能である。16ビット×16ワードのFIFOを備えている。また，レジスタ設定によりデクリプション入出力インターフェースを直結可能である。この場合はバッファの遅延のみとなる。

4.4 VR Parser

暗号化処理系，復号化処理系それぞれにVR parserを備える。VR parserはPack headerやPacket headerの解析を行い，ストリームデータから必要な情報を取得する。処理されるデータの単位は2048バイトである。

4.5 Decryptor

Decryptorはビットストリーム処理部，MKB処理部，タイトル鍵処理部，暗号処理部で構成されている。図2にDecryptorの内部構成を示す。図2(a)はMKB処理時のデータの流れを，図2(b)は再生ストリームデータ処理時のデータの流れをあらわしている。

4.5.1 データインターフェース

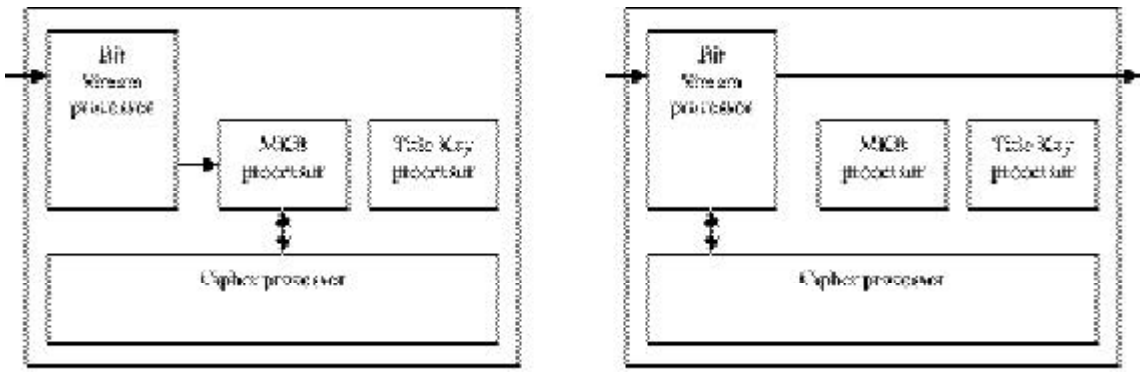
Decryptorは，データ入出力ポートをそれぞれ1系統備える。入力ポートには，MKBデータと再生ストリームデータが入力される。これらのデータは，ビットストリーム処理部で，Decryptorの内部処理に適した形式に変換され，取り込まれる。出力ポートからは，再生ストリームデータが，ビットストリーム処理部で形式を変換された後，出力される。

4.5.2 暗号処理

CPRMに必要とされるすべての暗号処理を暗号処理部で行なっている。暗号処理部は，演算部とそれに接続する複数のレジスタで構成されており，Decryptor内の他のブロックが発行する暗号処理命令に従って，演算部への演算命令の生成とレジスタの入出力制御を行ない，暗号処理を実行する。

4.5.3 MKB処理

MKB処理時には，MKB処理部がビットストリーム処理部及び暗号処理部を制御する。MKBは可変長のデータブロックの集合である。MKB処理部は，ビットストリーム処理部にデータを要求し，入力されたMKBデータからデータブロックの種別とブロックサイズを取得する。続いてデータブロックの種別に応じてデータ本体の処理を行なう。このとき必要であれば暗号処理部へ処理命令とともにデータを引き渡す。不要なブロックまたはデータが存在する場合は，次ブロックまでのデータをビットストリーム処理部に要求し，次のデータブロックの処理に移行する。このようにしてデータブロック単位での処理を繰り返すことで，暗号処理部の内部レジスタにメディア鍵が生成される。その後，このメディア鍵を検証し，正しいことが確認されると，MKB処理の完了をCPUに通知する。また，生成したメディア鍵が無効であったり，すべて



(a) MKB処理　　(b) ストリームデータ処理

図2　Decryptorブロック

のMKBデータを処理したにも関わらず正しいメディア鍵が算出されない場合には，CPUにその内容を通知して処理を終了する。

4.5.4 タイトル鍵生成

MKB処理の結果，正しいメディア鍵が得られると，タイトル鍵処理部が起動する。タイトル鍵処理部は，メディア鍵からタイトル鍵を生成するまでの処理を行なう。タイトル鍵は，メディア鍵とディスクに記録されている数種の情報から生成される。実際の演算処理は，タイトル鍵処理部の発行する命令に従って暗号処理部で行なわれる。生成されたタイトル鍵は暗号処理部の内部レジスタに格納される。

4.5.5 ストリームデータ処理

暗号化された再生ストリームデータを処理する際には，ビットストリーム処理部が暗号処理部を制御し，データの復号を行なう。暗号化されていないストリームデータは，ビットストリーム処理部からそのまま外部に出力され，Decryptorをバイパスする。ストリームデータの暗号化の有無は，VR Parserで判断され，Decryptorに通知される。データ復号の準備として，ビットストリーム処理部は，暗号処理部にコンテント鍵の生成命令を発行する。コンテント鍵は，VR Parserが再生ストリームデータから取得した情報とタイトル鍵を用いて，暗号処理部で生成され，データ復号時の鍵として使用される。コンテント鍵生成の後，ビットストリーム処理部は，暗号処理部に復号化命令とともにデータを送出し，結果を暗号処理部から受け取り，再生ストリームデータとして外部に出力する。

4.6 Encryptor

図3にEncryptorの内部構成を示す。EncryptorはDecryptorからMKB処理部とタイトル鍵処理部を省いたもので，ビットストリーム処理部と暗号処理部とで構成されている。Encryptorのビットストリーム処理部，暗号処理部は，Decryptorで使用されているものから不要な機能を省き，暗号化に対応させたものである。記録ストリームデータを暗号化するか否かは，VR Parserで判断され，Encryptorに通知される。暗号化しない記録ストリームデータは，ビットストリーム処理部からそのまま外部に出力される。ストリームデータを暗号化する場合，ビットストリーム処理部は，データ暗号化の準備として暗号処理部にコンテント鍵の生成命令を発行する。コンテント鍵はデータ暗号化時に鍵として使用される。コンテント鍵は，VR Parserが記録ストリームデータから取得した情報とDecryptorで生成したタイトル鍵を用いて，暗号処理部で生成される。コンテント鍵生成の後，ビットストリーム処理部は，暗号処理部に暗号化命令とともにデータを送出し，結果を暗号処理部から受け取り，記録ストリームデータとして外部に出力する。

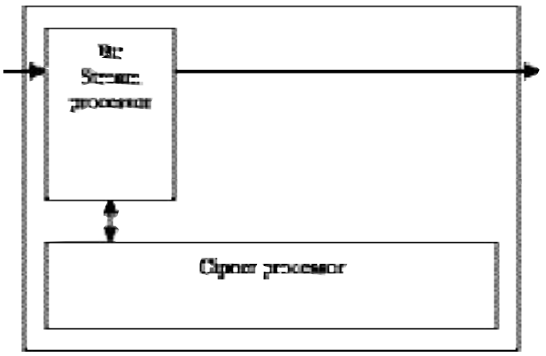


図3 Encryptorブロック

5. まとめ

DVD録画機で商用コンテンツを適正に記録するため，CPRMに準拠したコンテンツの暗号化，復号化を行なうCPRM LSIを開発した。

CPRM LSIは，暗号化処理系と復号化処理系を個別に備えることで，録再同時動作に対応した。また，暗号処理に必要な機密情報の守秘性を確保するため，ストリームデータの暗号化，復号化処理に加え，MKB処理，各種鍵の生成処理をハードウェアで実現した。さらに，ストリームデータを解析するVR Parserを内蔵した

ことで,ソフトウェアの介在なしにストリームデータから必要な情報を取得することを可能とし，CPRM 実装に伴うソフトウェアの負荷を抑制した。

今後も積極的に著作権保護に関する技術開発を推進し,著作権者と消費者の双方に理解される商品を開発して行きたいと考えている。

筆 者

山口 聡 (やまぐち さとし)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1990 年 4 月
- c.CD-R,DVD,DVD-R/RW 用LSI の開発に従事。

吉田 成孝 (よしだ しげたか)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1993 年 4 月
- c. DVD-R/RW 用LSI，DVD-R/RW ディスク用プリフォーマッタの開発に従事。

鈴木 敏雄 (すずき としお)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1980 年 4 月
- c. レーザディスク，DVD などの LSI 開発，DVD-R/RW 物理フォーマット開発及び規格策定に従事。

佐々木 努 (ささき つとむ)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1991 年 4 月
- c. 入社後，DVD-R/RW 用LSI 開発，Video Watermark の研究・開発に従事

河原 哲也 (かわはら てつや)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1992 年 4 月
- c. 入社後，システム商品の設計，Video Watermark の研究・開発に従事
- d. 専門分野：デジタル・アナログ論理回路設計

遠藤 秀人 (えんどう ひでと)
- a.研究開発本部 AV開発センター デジタル AV システム開発部
- b.1999 年 4 月
- c. 入社後，Video Watermark の研究・開発に従事
- d. デジタル回路設計