FPGAを用いたコンテンツ保護システムの設計と開発

横山浩之[†] 堀 洋平[††] 戸田賢二[††]

FPGAの動的部分再構成を利用し，デジタル信号処理機能の一部を外部ネットワークからプログラマブルに提供するセキュアなコンテンツ保護システムを提案するとともに，その具体的な応用例として，蓄積型映像配信サービスを想定したシステムを試作し，動作を検証した．本システムでは起動時に再構成モジュールが構築されておらず，これをサーバから入手して結合することで初めてコンテンツの再生が可能となる．端末上の固定回路と再構成モジュールのインタフェースを端末ごとに変えることで，ハードウェアの噛み合わせ自体が端末認証の役割を果たす．また，コンテンツに応じて再構成モジュールを変えることで，たとえ再構成モジュールの回路データがクラックされても，その影響を特定コンテンツと特定端末の組合せに限定することができる．こうして，ハードウェアによる高い処理性能を実現しながら，著作権侵害技術の進歩に柔軟に対応して処理方法を変更することが可能である．

Design and Implementation of FPGA-based Content Protection System

Hiroyuki Yokoyama,[†] Yohei Hori[††] and Kenji Toda[††]

We propose a new architecture for a content protection system that conceals confidential data and algorithms in an FPGA as electrical circuits. This architecture is designed for a client-server type on-line contents distribution services. The key component of this architecture is the hardware security module that is dynamically configured on the FPGA and performs the signal processing such as certification and decryption for replaying digital contents. This module is composed of two different circuits. One is the content-specific circuit that is built from the configuration data generated by the server. This circuit is specialized for each item of digital content. The other is the terminal built-in circuit that is uniquely programmed and implemented for each terminal, and is not open for the others. The content-specific circuit properly works only if it is combined with the terminal built-in circuit of the authorized client. We prototype and demonstrate a proof-of-concept model of the FPGA-based content protection system applicable to embedded consumer electronics such as set top boxes and cell phones.

1. はじめに

ブロードバンドインターネットの普及と，PC・情報家電・携帯電話の高機能化によって，遠隔地にあるサーバから付加価値の高いコンテンツを入手し，対価を支払って楽しむライフスタイルが定着しつつある．たとえば，音楽を携帯プレイヤや携帯電話にダウンロードして再生する蓄積型の音楽配信サービスや，セット・トップ・ボックス（Set Top Box，STB）を用いてオンデマンドで映像を鑑賞するビデオ・オン・デマンド（Video on Demand，VoD）サービスの市場が大きく成長しつつある．

一方，端末の高速化・省電力化の要求に応えるため，アプリケーションが必要とする高度な機能の一部をカスタム化されたハードウェアで提供し，システム全体の機能と性能を向上させる方法が広く用いられている．その結果，ハードウェアの設計も複雑化しており，ハードウェアについても，ソフトウェアと同様に，製品出荷後に新機能を追加し，不具合を修復できる柔軟性が要求されるようになってきた．さらに近年では，リバースエンジニアリングやサイドチャネル攻撃を用いた著作権侵害技術の向上が著しく，初期の設計や実装の有効期間が，製品寿命を下回る場合も生じている．そのため，機能モジュールの設計・実装を事後的かつ動的に変更できることが，最終製品に対しても求められている．こうした要求に応える1つの方法として，CPLD（Complex Programmable Logic Device）や

† 株式会社 KDDI 研究所
KDDI R&D Laboratories Inc.
†† 独立行政法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

FPGA（Field Programmable Gate Array）等の論理プログラマブルデバイス（以下，FPGA で代表する）をシステムの一部に組み込むアプローチがある．

さらに，情報端末は，重要な個人情報を管理するとともに，付加価値の高いコンテンツを取り扱うための暗号・認証・課金等の処理を行う必要があり，コンピュータシステムとしての強固なセキュリティ[1]が要求されている．

こうした要求に応える方法として，データやアルゴリズムを FPGA に回路として秘匿する方法が研究されている[2)~5)]．プロセス技術の進展にともなって，FPGA はさらに高速化・大規模化・低価格化しており，組み込み機器においても，複雑な処理を高速に実行できる柔軟なアクセラレータとして利用することが可能になりつつある．こうした FPGA に対して，機密性の高いデータやアルゴリズムを外部回路として秘匿する方法は，アクセスの容易なストレージ領域に，機密情報やプログラムをファイルとして残すことがないという点で秘匿性に優れている．さらに，FPGA 内部へのアクセスは回路上の制限を受けるため，ソフト的に機能を提供する方法に比べて，侵入や改ざんはより困難であり，動作の解析も難しく，クラッキングへの耐性も高い．このように，データとアルゴリズムを FPGA にまとめて隠蔽するアプローチは，パフォーマンスとセキュリティの双方を向上させる手法として有望である．

本稿では，FPGA の特性を最大限に活用するためのシステムアーキテクチャとして，端末固有回路（Terminal Built-in Circuit，TBC）とコンテンツ固有回路（Content-Specific Circuit，CSC）の 2 つのコンポーネントを FPGA 内部で結合してハードウェアセキュリティモジュール（Hardware Security Module，HSM）を構成し，この HSM の内部でコンテンツの復号や再生の処理を行うシステムを提案するとともに，その具体的な応用例として，VoD サービスを意識したコンテンツ保護システムを試作し，動作を検証する．

2. 関 連 研 究

システムのセキュリティを高める方法としては，プログラムを暗号化されたコードとして入力し，実行するための，特別なハードウェアを用いる手法が提案されている（ABYSS[6]，Citadel[7]，Dyad[8] 等）．これらのシステムは，コストが高く，システムアーキテクチャに柔軟性がないため，システムのメンテナンスが困難で，新しい著作権侵害技術に対抗するのは難しい．そうした問題を解決する方法として，FPGA を用いたセキュアプロセッサが提案されているが[9),10)]，これらのアプローチはいずれも，プログラムの実行コードや入出力データの難読性を高めることによって，セキュアなソフトウェア実行環境を提供することを目的としている．一方，本研究は，FPGA の内部において機密情報処理を回路的に行い，ソフトウェアが情報の内容を直接取り扱う機会そのものを減らすことによって，ウィルス等によるソフト的な攻撃を防ぐことを目的としている．FPGA を用いた著作権管理システムについての従来手法[11)]との相違は，部分的自己書き換えが可能な FPGA の特性を利用して，回路的な認証を行う手段を提供するとともに，回路を動的に再構成することでロジック設計の推測を困難にし，ハード的にシステムをセキュア化することを目指している点にある．

一方，PC 等の個人用計算機におけるセキュリティ標準は Trusted Computing Group（TCG）[12)]において策定されている．TCG のセキュリティメカニズムの中心は，Trusted Platform Module（TPM）と呼ばれるセキュアチップであり，周辺装置や OS を含む，プラットフォーム全体の完全性を保証する機能を提供するが，TPM 自体がコンテンツ保護機能を提供するわけではない．

著作物の不正コピーを防止し，ライセンスを適切に管理するデジタル著作権管理システム（Digital Right Management System，DRM）についても多くの研究がなされており[13),14)]，Content Protection for Recordable Media（CPRM）[15)]，High-Bandwidth Digital Content Protection（HDCP）[16)]，Digital Transmission Content Protection（DTCP）[17)]，High Definition Multimedia Interface（HDMI）[18)] 等の仕様が標準化されている．本研究は，これらの技術に対抗するものではなく，むしろ，これらの機能をより安全かつ柔軟に実装するための枠組みを提供するという位置付けにある．たとえば，HDMI に準拠する動画像用インタフェース機能を FPGA に取り込むことにより，画像表示装置への出力信号を，FPGA 内部で暗号化することができる．この方法の利点は，オリジナルデータが外部回路にいっさい露出せずに，コンテンツの復号から再生までの処理を一貫して実行できること，および，表示装置の交換やインタフェース仕様の更新について柔軟に対応できることにある．

なお，セキュリティを提供するハードウェアモジュールに対しては，チップ自体にも耐タンパ性[19)]が要求されており，特にサイドチャネル攻撃への対策は重要であることが知られている[20)]．しかし本稿は，部分書き換えを用いたセキュア化技術の検討を主目的とし，

使用するチップの耐タンパ性に関連する検討は今後の課題とする．

3. コンテンツ保護システムの構成

3.1 コンテンツ保護システムの基本構成

ネットワークを経由してオンデマンドで映像等のデジタルコンテンツを配信する蓄積型の VoD サービスを提供する場合，コンテンツが不正に利用されることを防止するために，サーバからクライアント端末への通信経路に暗号を施し，第三者による盗聴を防止する方法や，コンテンツを暗号化して複製による不正利用を防止する方法が用いられている．ここで，前者の暗号化を「経路暗号化」，後者の暗号化を「コンテンツ暗号化」と呼ぶ．これらの暗号化に対しては，DES [21]，Triple DES [22]，AES [23),24)] 等の既知の方式が利用できる．暗号を解くための鍵の交換に関しては RSA 公開鍵暗号法[25)] 等が利用できる．ただし，端末におけるアプリケーションソフトや OS がクラックされたり，データバスの信号が測定された場合，復号に必要な鍵（復号鍵）や，復号された後の平文コンテンツデータを盗み出される恐れがある．こうした問題を解決する 1 つの方法は，復号鍵と復号処理の双方を同一の FPGA 内に回路として構築することである．この方法は，復号鍵，復号途中のデータ，および復号後の平文データが，まったく外部回路に露出しないため，ソフトウェアの改変やバス信号の測定を用いた攻撃に対する耐性は高い．

回路によってアルゴリズムやデータを秘匿し，コンテンツを不正利用から守るコンテンツ保護システムの基本構成を**図 1** に示す．図 1 のシステムは，サーバ，クライアント端末，およびそれらを接続するネットワークから構成されている．ここでクライアント端末は，汎用の PC ではなく STB 等の専用の端末を想定する．

端末からサーバに対してデジタルコンテンツのダウンロードが要求されると，サーバは，暗号化されたコンテンツを端末が処理するために必要な回路の一部を作成する．これをコンテンツ固有回路（Content-Specific Circuit，CSC）と呼ぶ．CSC は，要求元の端末に用意されている端末固有回路（Terminal Built-in Circuit，TBC）と結合することで初めて正しく動作するように作成される．この CSC の回路情報は暗号化され，コンテンツとともに，ネットワーク経由で端末に送信される．

端末は CSC の回路情報を復号し，FPGA 上で CSC と TBC を合成してハードウェアセキュリティモジュール（Hardware Security Module，HSM）を構築する．この HSM に暗号化コンテンツを入力し，必要な信号処理を行う．デジタルコンテンツの種類としては，書籍等の文字情報，静止画像，音声や音楽，動画像，およびそれらの組合せが想定される．そのため，所望の出力を得るには，コンテンツの種類に応じたインタフェース機能が必要となる．たとえば，VoD サービスを考えた場合，NTSC（National Television Standards Committee），DVI（Digital Visual Interface），HDMI [18)] 等のビデオ出力形式に対応する必要がある．ここで，MPEG-2 等のデコーダ（伸張回路）に加えて HDMI 等のインタフェース回路を HSM の内部に用意すれば，ビデオ出力も含めて，不正利用が容易な形式でコンテンツデータが露出することはなくなる．

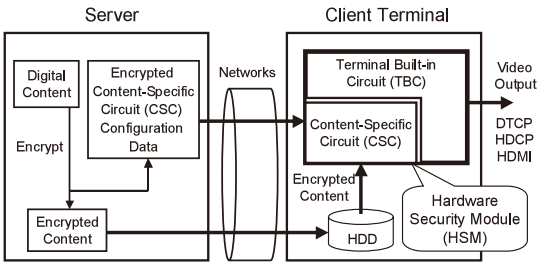

図 1 コンテンツ保護システムの基本構成
Fig. 1 Functional architecture of content protection system.

このシステムでは，CSC が攻撃対象になりうるが，回路情報は暗号化して送信されるので，解読は困難である．また，仮に解読されたとしても，CSC の回路情報はネットリストの形式であり，ソフトウェア的に意味のあるものではなく，しかも単体では回路として正常に動作しない．そのため，TBC の情報を持たない第三者にとっては，CSC の回路情報から HSM 全体を推測することは困難である．

このように，提案システムを用いることによって，端末に送付されたデータが流出したとしても，第三者による不正利用を困難にすることができる．

3.2 クライアント端末の装置構成

クライアント端末は，利用形態に応じて様々な回路構成をとることができる．本節ではいくつかの構成例を取り上げ，それぞれの特徴について述べる．

最も基本的な構成を**図 2** に示す．端末は，ディスク装置，CSC，TBC，MPEG 伸張回路（MPEG Decoder），ビデオ出力回路（Video Adapter）で構成されている．

CSC は，復号回路（Decrypter）と動作制御回路（Circuit Controller）から構成されている．復号回路

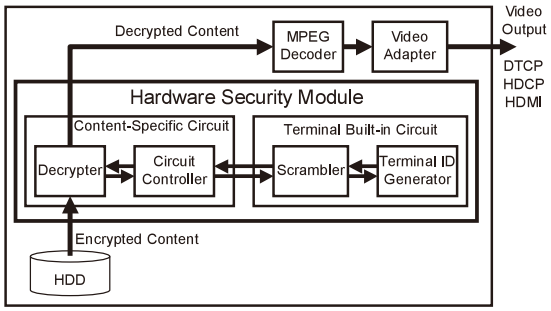

図 2 クライアント端末装置構成例 1
Fig. 2 System configuration of a client terminal: Type-1.

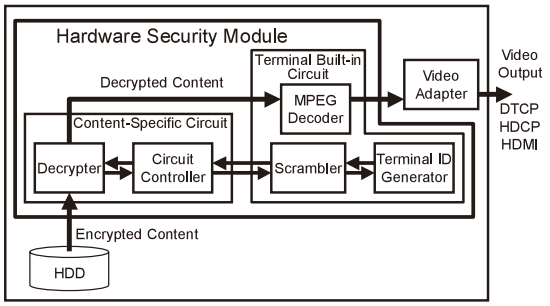

図 3 クライアント端末装置構成例 2
Fig. 3 System configuration of a client terminal: Type-2.

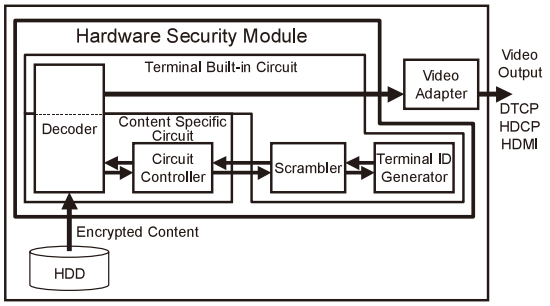

図 4 クライアント端末装置構成例 3
Fig. 4 System configuration of a client terminal: Type-3.

は，暗号化コンテンツを元のデジタルコンテンツに復元する回路である．動作制御回路は，CSC と TBC の組合せが正しい場合にのみ復号回路を動作させることができる．また，動作制御回路は，デジタルコンテンツの再生に何らかの条件がある場合は，その条件を満足する場合に限って復号回路を動作させる．たとえば，コンテンツの再生期間が制限されている場合，動作制御回路は，端末装置のタイマを読み出し，現在の日時が再生期間内である場合に限って復号回路を動作させる．

TBC は，端末 ID 出力回路（Terminal ID Generator）とスクランブル回路（Scrambler）から構成されている．端末 ID 出力回路は，端末に固有のビット列を出力し，スクランブル回路は，その端末 ID を，コンテンツに固有の情報を用いて攪拌する．たとえば，端末 ID 出力回路が 256 ビットの端末 ID を出力し，スクランブル回路が，この端末 ID と，256 ビットの 2 進数で表されるコンテンツのハッシュ値との排他的論理和をとり，その値を乱数の種として 256 ビットの疑似乱数を 256 個生成する．こうして生成された疑似乱数のうち，最後に得られた乱数の値を攪拌端末 ID として出力する．動作制御回路は，この出力値が回路内にあらかじめ設定された値と一致した場合に限って，復号回路を作動させるといった制御を行うことができる．

ただし，HSM と MPEG 伸張回路をつなぐデータ線が測定されると，復号された平文データが取り出される危険性がある．

図 3 における構成例 2 は，MPEG 伸張回路が TBC の一部として構成されることを特徴としている．この構成例では，HSM の内部で暗号化コンテンツの復号および伸張を行うことによって，復号された状態の，MPEG-1 や MPEG-2 等の規格に準拠した動画像データが FPGA の外部に出力されることを防止できる．ただし，復号回路と MEPG 伸張回路との間のデータのやりとりは，OS を介在することなく直接行われるように端末システムの設計および実装を行う必要がある．

なお，復号回路と MPEG 伸張回路を実装するにあたっては，FPGA ではなく専用回路を用いても，平文コンテンツが露出することを防止できる．しかし，FPGA で実装すれば，TBC のアップデートによって，画像圧縮の方式に関する修正や改良を行ったり，CSC をコンテンツに応じてカスタマイズしたりすることで，鍵長や暗号方式を変更し，さらなる不正コピー耐性を得るといったメリットがある．

図 4 における構成例 3 は，復号回路と MPEG 伸張回路が一体的に構成されている点に特徴がある．すなわち，復号・伸張回路は，その一部が CSC に構築され，残りが TBC に構築されている．この構成では，復号や MPEG のデコードに使われる典型的な論理演算ブロックを TBC に配置し，それらに対するパラメータや，補助的な回路を CSC に配置するといった，柔軟な構成をとることができる．また，デジタルコンテンツの復号処理と MPEG のデコード処理を一体的に行うことで処理を効率化することや，TBC の推定をより困難にする工夫が可能となっている．

図 5 における構成例 4 は，MPEG 伸張回路とビデオ出力回路が TBC の一部となるように構成されることを特徴としている．この場合，暗号化コンテンツに対する復号処理と伸張処理だけでなく，表示可能な状

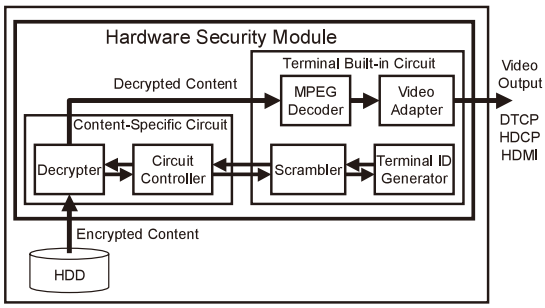

図 5 クライアント端末装置構成例 4
Fig. 5 System configuration of a client terminal: Type-4.

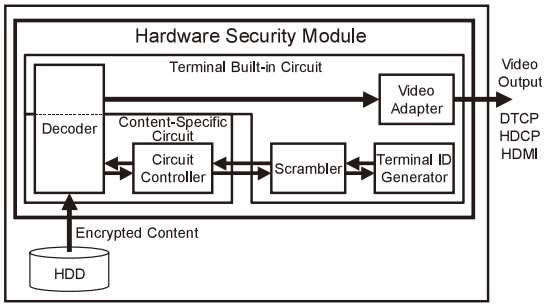

図 6 クライアント端末装置構成例 5
Fig. 6 System configuration of a client terminal: Type-5.

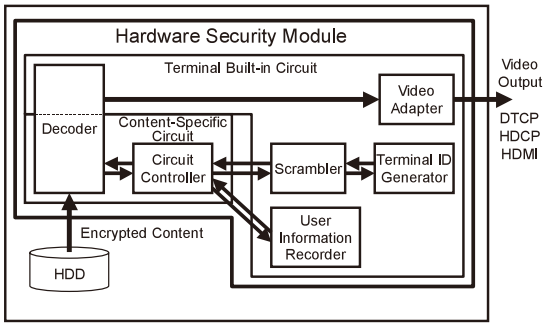

図 7 クライアント端末装置構成例 6
Fig. 7 System configuration of a client terminal: Type-6.

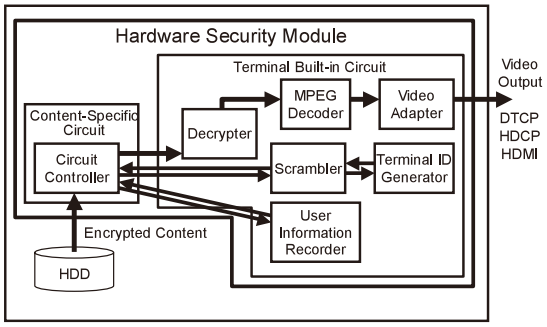

図 8 クライアント端末装置構成例 7
Fig. 8 System configuration of a client terminal: Type-7.

態となったコンテンツを最終的な表示デバイスに出力するまでのすべての処理を，FPGA の内部に閉じた状態で行うことができる．さらに，HDMI 等の規格に対応することで，デバイス間で相互認証を行い，映像データをデバイス間で暗号化して伝送することによって，より強力にコンテンツ保護することも可能となる．

図 6 における構成例 5 は，復号回路と MPEG 伸張回路が復号・伸張回路として一体的に構成されるとともに，ビデオ出力回路が TBC の一部となるように構成されることを特徴としている．図 4 で示したクライアント構成例 3 と同様に，デジタルコンテンツの復号処理と MPEG のデコード処理を一体的に行うことが可能である点に加え，構成例 4 と同様に，コンテンツのデジタルデータが露出することなく，最終的な表示デバイス向けのビデオ信号のみを外部に出力できる点で，コンテンツ保護の強度は高い．

図 7 における構成例 6 は，デジタルコンテンツの再生回数や再生期間等の利用者の状況に関連した情報を記録する回路（ユーザ情報記録回路）を TBC に取り入れた構成となっている．たとえば，コンテンツの再生回数に制限がある場合，動作制御回路は，TBC 内にあるユーザ情報記録回路に，暗号化コンテンツのハッシュ値と再生回数の制限数を与える．ユーザ情報記録回路は，暗号化コンテンツのハッシュ値に対応する再生回数残余カウンタをチェックし，そのカウンタが未定義であれば，再生回数の制限数で初期化する．再生回数残余カウンタが 1 以上であれば，ユーザ情報記録回路は再生回数残余カウンタを 1 つ減らすとともに，動作制御回路にコンテンツの再生が可能であることを通知する．もし再生回数残余カウンタがゼロ以下であれば，動作制御回路にエラーを通知し，動作制御回路は CSC を停止させる．

図 8 における構成例 7 は，復号・伸張回路を TBC の一部となるように変更し，CSC は，復号回路の動作制御と，暗号化データを復号回路に入力するためのインタフェース機能の提供に特化している点に特徴がある．構成例 7 は構成例 6 から派生したものだが，同様の変更は構成例 1，2，4 に対しても可能である．

4. コンテンツ保護のメカニズム

コンテンツ再生時に CSC を動的に構成し，TBC と結合させる CSC-TBC 結合アーキテクチャは，セキュアな認証のメカニズムを回路的に提供できる点に特徴がある．たとえば，ザイリンクス社の FPGA において，部分書き換えを行うモジュール間の通信を保証するには，モジュールの境界を通過するすべての信号が，

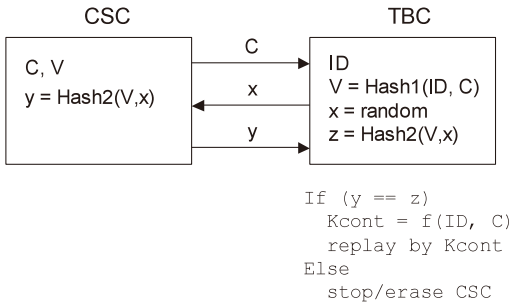

図 9 チャレンジレスポンス方式による回路認証
Fig. 9 Challenge-response authentication for CSC-TBC interlocking mechanism.

バスマクロ[26]と呼ばれるコンポーネントを通じてやりとりされる必要がある．もし，それらのバスマクロが正しい場所に配置されていなければ，CSC が再構成されたときに，回路全体が正常に動作することはない．

ここで，CSC と TBC の 2 つの回路が正しく結合し，全体として設計どおりに動作することを，ハードウェアが噛み合わされるという意味で**インターロックする**という．CSC-TBC がインターロックするには，CSC-TBC 間で以下の条件がすべて成立する必要がある．

(1) 空間的条件：接続配線の位置が一致する．
(2) 時間的条件：送受信される信号のタイミングが適合する．
(3) 電気的条件：接続配線における電圧や電流等の条件が適合する．
(4) 論理的条件：プロトコルが一致し，送受信されるデータが適合する．

以上の条件を CSC-TBC 間の組合せに固有のものとすることにより，インターロックを認証の手段として利用することができる．

論理的条件のプロトコルの一例として，チャレンジレスポンス方式を取り入れた例を**図 9** に示す．図中の TBC 内には，端末固有の ID，1 方向関数 $Hash1$ および $Hash2$，鍵生成関数 f が埋め込まれている．サーバからは，コンテンツ識別子 C，1 方向関数 $Hash2$，認証用のパラメータ V を含む回路情報が CSC 内に回路として与えられる．TBC は乱数 x を生成して CSC に送る．CSC は x をもとに $y = Hash2(V, x)$ を計算し，TBC に返送する．TBC は $z = Hash2(V, x)$ を計算して y と比較し，両者が一致すれば，コンテンツを復号するための鍵 Kcont を生成し，再生を開始する．このように，乱数 x を用いて CSC-TBC 間での情報交換を行うことによって，上記 4 つの条件がすべて成立することを確認できる．コンテンツ鍵 Kcont を時間とともに更新する場合は，そのつど，チャレンジレスポンスを行うことで，より確実に CSC の検証を行うことができる．

さらなるセキュア化のためには，CSC-TBC のインターロックが失敗した回数を記録し，所定の回数に達した場合は，CSC の再構成禁止，TBC の消去，HSM の一時停止等を行うことにより，不正な CSC 構成データを用いた攻撃を抑止することができる．

5. システムの実装

CSC-TBC のメカニズムを，ハイビジョン動画像の再生システムに応用した場合を想定してシステムの実装を行った例を示す．

5.1 システムのハードウェア構成

本稿では，試作システムを設計するうえでの目標を，以下の 2 つに定めた．

(1) 復号処理と符号化処理を 1 つの FPGA 内で行うことにより，平文コンテンツデータをチップ外に露出させない回路構成を実現する．
(2) 1 つの機能を複数の回路にまたがって実装することの有効性を確認する．

一方，使用する FPGA の容量および回路設計に要する工数を最小限にするため，ビデオ出力については既存の回路を外部接続して使用することとした．そのため，試作システムは，図 4 における構成例 3 のアーキテクチャに基づく回路構成とした．

設計した回路を実装するためのボードとして，レクセオン・テクノロジー社☆ の REX2（REconfigurable EXperimental equipment 2）を用いた．REX2 は，ザイリンクス社の FPGA，Virtex-II Pro XC2VP70[27] を 1 個搭載した FPGA 開発ボードである．REX2 を用いた検証システムのハードウェア構成を**図 10** に示す．検証システムは，CSC-TBC メカニズムや動画再生回路が実装される主ボード（REX2 MAIN），PC から映像ソースを供給するための PCI-X ボード（REX2 PCI-X），および DVI 入出力ボード（REX2 DVI）から構成される．

Virtex-II Pro には，自己書き換えを行うための ICAP（Internal Configuration Access Port）[28] と呼ばれる内部ポートがある．これを利用することで，外部回路を使わずに自らの制御で CSC を構築することが可能になる．Virtex-II Pro では，部分書き換え対象となるモジュールと固定モジュールの間の信号をバ

☆ レクセオン・テクノロジー（株）は，（独）産業技術総合研究所の技術移転により設立されたベンチャー企業である．
http://www.rexeon.com/

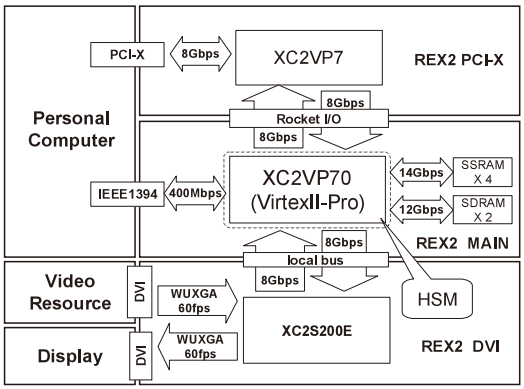

図 10 検証システムのボード構成
Fig. 10 Board configuration of the prototype system.

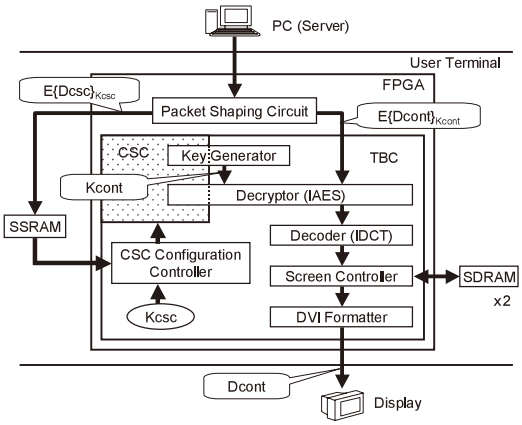

図 11 検証システムのアーキテクチャ
Fig. 11 Block diagram of the prototype system.

スマクロ経由にすることで，部分書き換えの前後での信号の結線が保証される．本システムでは，TBC のバスマクロの配置は，あらかじめ固定されている．ゆえに，動的に再構成される CSC のバスマクロの配置が TBC と完全に一致することがインターロックするための空間的条件となる．

5.2 検証システムの内部構成

図 11 に検証システムのアーキテクチャを示す．端末がコンテンツの配信を要求してから動画像が再生されるまでの全体的な動作は次のとおり．端末はサーバに対して，再生したいコンテンツの識別子を指定する．サーバは，端末がそのコンテンツを再生するのに必要な CSC を生成し，その CSC とコンテンツをそれぞれ暗号化して端末に配信する．端末は，受信した暗号化 CSC データを使って，FPGA 上に CSC-TBC 結合回路を構築する．この回路が生成する復号鍵を用いて，暗号化された動画像コンテンツを復号し，オリジナルの平文コンテンツデータを得る．この平文データをビデオ映像に変換して外部モニタへ出力する．

ここで，提案システムは，端末を提供する事業者が ASP（Application Service Provider）としてコンテンツ配信サービスを提供することを仮定する．すなわち，サーバには，すべての端末における TBC の情報があると仮定する．コンテンツを提供する事業者は，コンテンツ配信サービス提供者に対してコンテンツを提供し，コンテンツ配信サービス提供者が，端末に対してコンテンツを提供する．

以下，本システムの動作を詳細に説明する．データ D を暗号化したものを $E\{D\}$ で表し，鍵 K を明示する場合は $E\{D\}_K$ と表す．

まず，端末は次のように動作する．

(1) システムを起動し，FPGA 上に TBC を構築する．

(2) サーバに対して，コンテンツ識別子 C_1 のコンテンツを要求する．

次に，要求を受けたサーバは以下のとおり動作する．

(3) 端末を認証し，コンテンツ C_1 を提供できることを確認する．

(4) 端末に固有の秘密鍵 K_{CSC} と，端末固有回路 TBC の内容に関する情報をデータベースから得る．

(5) 乱数によって Dseed と C_3 を設定し，CSC の再構成データ D_{CSC} を作成する．

(6) 秘密鍵 K_{CSC} を用いて D_{CSC} を AES 方式で暗号化し $E\{D_{\mathrm{CSC}}\}_{K_{\mathrm{CSC}}}$ を得る．

(7) CSC と TBC の内容に基づいて，CSC-TBC 結合回路が生成するコンテンツ鍵 Kcont を計算する．

(8) Kcont を用いてコンテンツのオリジナルデータ Dcont を AES 方式で暗号化し，$E\{D\mathrm{cont}\}_{K\mathrm{cont}}$ を生成する．さらに，$E\{D\mathrm{cont}\}_{K\mathrm{cont}}$ を 64 ビットごとに区切り，それぞれに対して 5 ビットの左循環シフトを行ったのち，$H_2(C_3)$ との排他的論理和をとって $H\{E\{D\mathrm{cont}\}_{K\mathrm{cont}}\}$ を生成する．

(9) $E\{D_{\mathrm{CSC}}\}_{K_{\mathrm{CSC}}}$ と $H\{E\{D\mathrm{cont}\}_{K\mathrm{cont}}\}$ を端末に送信する．

サーバから $E\{D_{\mathrm{CSC}}\}_{K_{\mathrm{CSC}}}$ と $H\{E\{D\mathrm{cont}\}_{K\mathrm{cont}}\}$ を受信した端末は，次のように動作する（図 11 参照）．

(10) $E\{D_{\mathrm{CSC}}\}_{K_{\mathrm{CSC}}}$ を SSRAM に蓄積する．

(11) 秘密鍵 K_{CSC} を用いて，SSRAM 内の $E\{D_{\mathrm{CSC}}\}_{K_{\mathrm{CSC}}}$ を CSC 復号回路によって復号する．

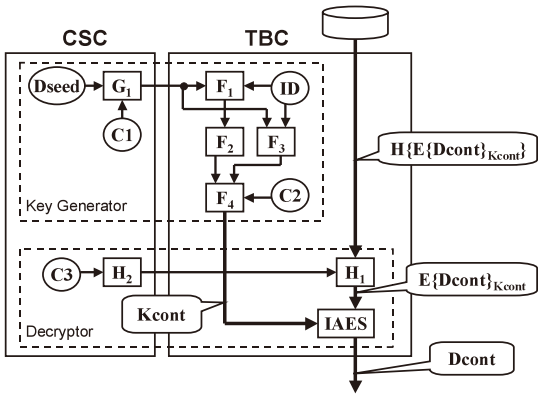

図 12 検証システム内部のブロック図
Fig. 12 Block diagram of the CSC-TBC interlocking part.

(12) 復号された D_{CSC} を用いて部分書き換えを実行し，CSC を構成する．
(13) CSC-TBC 結合回路でコンテンツ復号鍵 Kcont を生成する．CSC が TBC と正しく結合（インターロック）すると正しい鍵が生成され，そうでない場合は，誤った鍵が生成される．
(14) コンテンツデータに対するバイナリ逆変換および復号処理を行う．復号鍵 Kcont が正しければ，コンテンツは正しく再生される．

図 12 に CSC-TBC のインターロック部のより詳細なブロック図を示す．ここで，CSC は機能ブロック G_1 および H_2 を担当し，TBC は機能ブロック F_1〜F_4，H_1，および $IAES$（AES の復号）を担当する．コンテンツを再生するには，AES（CBC mode，128-bit block size，128-bit key）を復号するための鍵 Kcont の生成と，バイナリ変換 H を行う必要があり，それぞれに対して，TBC および CSC の回路に固有の情報や機能が必要となっている．

本検証システムの目的は，CSC-TBC メカニズムのコンセプトを実証することにある．特に，今回の実装では，インターロックの成否を利用したコンテンツ保護が正しく機能するかどうかを確認することを重視している．そのため，CSC-TBC で実行するデータ処理としては，以下に示す簡易な関数を用いた．

$$F_1 = (ID + G_1) <<< 64$$
$$F_2 = TABLE(F_1)$$
$$F_3 = (ID <<< 16 + G_1) <<< 32$$
$$F_4 = F_2 + F_3 + C_2$$
$$G_1 = D\mathrm{seed} <<< 96 + C_1$$
$$H_2 = C_3$$

ここで，演算子 + は排他的論理和を表し，<<< は左循環シフトを表す．$TABLE(i)$ は，アドレス長 8 ビット，データ長 128 ビットのテーブルを，アドレス i で参照する関数を表す．バイナリ変換 H_1 は，$H\{E\{D\mathrm{cont}\}_{K\mathrm{cont}}\} + H_2(C_3)$ を 64 ビットごとに区切り，それぞれに対して 5 ビットの右循環シフトを行う演算である．これらの関数は，データの難読化を実現するよりむしろ，典型的な演算を組み合わせることによって実際の回路規模を大まかに模擬することを目的としている．また，ID は端末を一意に特定できる端末識別子，Dseed および C_3 は新たにコンテンツが要求されるごとに更新される乱数，C_1 はコンテンツ識別子，C_2 はファームウェアアップデート時に更新される乱数である．また，端末に固有の秘密鍵 K_{CSC} は，出荷時に，TBC の内部において設定されるものとする．

表 1 端末固有回路（TBC）の回路使用率
Table 1 Hardware resource utilization of TBC.

Resource	Utilization	(%)
SLICEs	11,881 / 33,088	36%
Block RAMs	235 / 328	72%
MULT18x18s	53 / 328	16%
BUFGMUXs	7 / 16	43%
DCMs	7 / 8	88%
ICAPs	1 / 1	100%

表 2 コンテンツ固有回路（CSC）の回路使用率
Table 2 Hardware resource utilization of CSC.

Resource	Utilization	(%)
SLICEs	311 / 33,088	1%

5.3 実装結果

回路の作成は，ザイリンクス社の統合開発環境 ISE8.1i[29] を用いて行った．また，フロアプランには同社の PlanAhead 8.2.3[30] を使用した．ターゲットデバイスは Virtex-II Pro XC2VP70 である．

TBC および CSC のハードウェアリソースの使用量を，それぞれ**表 1** および**表 2** に示す．CSC の大きさは，生成されるビットストリームのサイズが最小となるように決定した．これらの表が示すように，CSC が使用する SLICE 数は TBC と比較してきわめて少なく，回路のごく一部分のみを変えることで，セキュアで粒度の細かな保護システムを提供可能であることが分かる．FPGA 全体の回路構成データが約 3.6 MB であるのに対し，CSC の暗号化ビットストリームは約 75 KB と，およそ 1/50 の大きさである．CSC の再構成データはネットワークを経由して送信されるが，ネットワーク負荷は小さく，ダウンロード時間も短いといえる．

6. システムの検証実験

CSC-TBC によるコンテンツ保護のメカニズムを FPGA 上に実装し，実際に部分書き換えを行って動作を検証した．CSC-TBC の保護メカニズムは，暗号化された 1080p ハイビジョン（1920×1080 ピクセルのプログレッシブモード）の動画像が正しく再生できるかどうかで検証した．

6.1 実験方法

バスマクロの配置が異なる 2 つの端末，A および B を用意するとともに，それぞれの端末において，正常に動画が再生されるように，CSC と暗号化された動画のペアを作成する．これを（CSC-A1，動画 1）および（CSC-B1，動画 2）とする．ここで，5.2 節で述べた手順を以下の条件で実行する．

A) 端末 A で CSC をまったく構築していない状態（システム初期状態）のまま動画 1 を再生．
B) 端末 A で CSC-A1 を構築し，動画 1 を再生．
C) 端末 B で CSC-A1 を構築し，動画 1 を再生．
D) 端末 A で CSC-A1 を構築し，動画 2 を再生．
E) 端末 B で CSC-A1 を構築し，動画 2 を再生．

6.2 実験結果

A) の CSC が構築されていない状態では，**図 13** に示すように映像が砂嵐状に再生された．これは，CSC が構築されなければ正しい鍵が生成されず，コンテンツの復号に失敗することを表している．よって，端末が盗難によって第三者の手に渡った場合でも，コンテンツを再生するための CSC を入手できなければ，再生は不可能である．CSC の入手を PIN（Personal Identification Number）等で制限していれば，端末の盗難・紛失時にコンテンツが不正ユーザに利用されることを防ぐことが可能である．

B) は CSC と TBC がインターロックされた状態であり，ユーザによってシステムが正しく利用された場合に相当する．このとき，コンテンツは**図 14** に示すように正しく再生された．これは，部分書き換えを利用した CSC の構築，CSC-TBC のインターロック，CSC-TBC による鍵の生成，およびコンテンツの復号に成功したことを表している．

C) は，対応のとれている CSC とコンテンツを，別の端末で再生しようとした場合に相当する．このとき，コンテンツは A) の場合と同様に砂嵐状に再生された．これによって，ネットワーク経由で配信されたコンテンツと回路情報 $E\{D_{\mathrm{CSC}}\}$ が盗聴され，かつ何らかの事情によって D_{CSC} が取り出された場合でも，別の端末では CSC がインターロックせず，コンテンツを正常に再生できないことが示された．

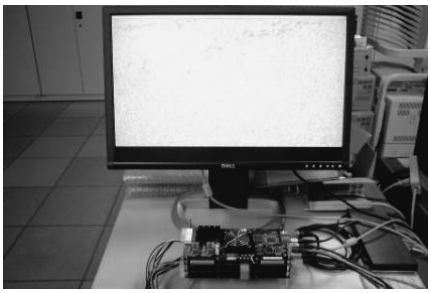

図 13 動画再生実験の結果（インターロック失敗時）
Fig. 13 The result of image replay testing where CSC and TBC failed to be interlocked.

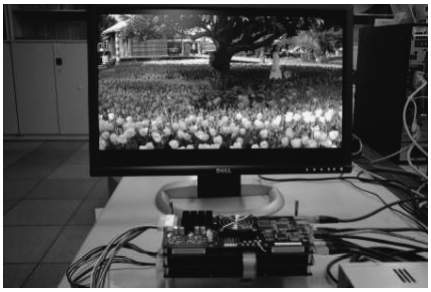

図 14 動画再生実験の結果（インターロック成功時）
Fig. 14 The result of image replay testing where CSC and TBC are successfully interlocked.

D) は，端末と CSC の対応はとれているが，CSC と対応するコンテンツとは異なるものを再生しようとした場合に相当する．このとき，コンテンツは A) の場合と同様に砂嵐状に再生された．

E) は，ライセンスの失効等により CSC を入手できない状況において，他の端末の CSC を使ってコンテンツの再生を試みた場合に相当する．このときコンテンツは，A) の場合と同様に砂嵐状に再生された．

7. 考　　察

7.1 提案システムの安全性

提案システムの安全性について述べる．本システムが想定している攻撃は，第 1 に，特権モードで動作する悪意のあるソフトウェアによって，CPU レジスタ，メモリ，データバス等から，鍵や平文データを読み取るようなシステム的な攻撃であり，第 2 に，CSC を解読・分析・偽造する攻撃である．

第 1 の攻撃方法に対しては，FPGA の内部において機密情報の処理を回路的に行い，処理中の中間データや平文データを外部バスに出力しないことによって，ソフトウェアが機密情報を直接取り扱う機会そのものを減らし，安全性を高めることができる．FPGA に

表 3 クライアント端末装置構成例の機能比較
Table 3 Advantages and disadvantages of system configuration.

構成例	安全性	柔軟性	粒度	FPGAコスト	通信コスト	用途
構成例1	△	△	△	◎	○	省スペース携帯型プレイヤー
構成例2	○	△	△	○	○	携帯型プレイヤー
構成例3	○	○	○	○	△	ブロードバンド対応携帯型プレイヤー
構成例4	◎	△	○	△	○	パーソナルSTB
構成例5	◎	○	○	△	△	ブロードバンド対応パーソナルSTB
構成例6	◎	◎	◎	×	△	ブロードバンド対応STB
構成例7	◎	△	◎	×	◎	放送受信型ナローバンドSTB

対するサイドチャネル攻撃も重要な脅威であるが[20]，CSC や TBC の回路構成を定期的に変更することによって，解析結果の有効期間を短縮する対抗手段をとることができる．今後，FPGA の製造プロセスがさらに微細化し，チップ自体に耐タンパ性[19] が具備されるようになれば，サイドチャネル攻撃の有効性は，より低下する．

第 2 の攻撃方法に対しては，解読・分析・偽造の 3 つの観点で考える．

まず，CSC に対して攻撃を行うには，CSC の回路データに施された暗号を解読する必要がある．一方，CSC に対する暗号の強度は，通常，コンテンツに対するのと同程度の強度としている．よって，CSC の暗号を解読するには，コンテンツの暗号を解読するのと同程度のコストが必要である．

解読によって，CSC の回路データを分析することができたとしても，得られるのは，コンテンツの復号鍵を生成するための，回路の一部に関する情報のみであり，鍵そのものを取り出すことはできない．分析によって，仮に，CSC 内部のロジック，パラメータ，および特定の TBC との物理的なインタフェースが判明しても，TBC 内部に閉じたロジックおよびパラメータを推定し，復号鍵を得るのは困難である．

CSC の分析をもとに，他の端末において動作する CSC を偽造し，CSC をインターロックさせるには，少なくともバスマクロ[29] の配置や形状等に関する条件を，対象 TBC に適合させる必要がある．本試作システムで用いた FPGA の場合，1 つのバスマクロについて，縦方向 104 行，横方向 70 列，入出力の向き，バス形状の選択，同期・非同期の選択，バスマクロ内の信号 8 ビットの使用パターンに関する，$104 \times 70 \times 2 \times 2 \times 2 \times 2^8 = 1.49 \times 10^7$ 通りの組合せを一致させる必要がある．これに加えて，コンテンツと端末の組合せに対応した，論理的な結合条件を満たさなくてはならない．また，CSC 構築回路は，暗号化ビットストリームのみを受け付けるため，回路データを正しく暗号化する必要がある．バスマクロの配置や形状等の条件が一致しているか否かは，実際に CSC を構築してみないと分からないため，インターロックの失敗回数に上限のあるシステムでは，偽造された CSC がインターロックに成功する確率は小さい．

以上より，CSC の解読コストはコンテンツの解読コストと同等であり，CSC の分析によって得られる情報から鍵を推定することは難しく，他の端末でインターロックする CSC を偽造できる確率も小さい．したがって，第 2 の攻撃方法は有効性に乏しい．

7.2 提案システムの柔軟性と粒度

提案システムは，回路のアップデートによる修正や改良が可能である点に特長がある．この動的な機能変更の能力は，柔軟性と粒度の 2 つの軸によって評価することができる．

柔軟性は，機能変更の頻度に対応し，頻度が高いほど柔軟性は高くなる．提案システムにおいて，CSC はコンテンツを再生するごとに構築されるため，柔軟性の高い運用が可能である．一方，TBC の更新周期は比較的長くなるため柔軟性は低い．コンテンツ保護の観点から見た場合，著作権侵害技術によって攻撃されやすい機能については柔軟性を高め，防御手段を素早く展開できる方が望ましい．そこで，暗号方式については CSC でカスタマイズ可能とする一方，MPEG 伸張方式は TBC 側に用意し，新たな規格の導入に対してはファームウェアアップデートで対応するという方法が考えられる．

一方，粒度とは，変更可能な機能やパラメータの細かさを表す．暗号方式と鍵長を個別に変更したり，MPEG 方式のプロファイルやビデオ出力方式における様々なパラメータを個別に追加・変更・調整したりできる場合は粒度が細かい．ただし，粒度が細かいほど，回路は大規模化し，コンテンツ再生時の通信量や回路更新時間が増加する．

7.3 提案システムの構成例の特徴比較

以上をふまえて，3 章で述べた構成例の特徴を比較したものを**表 3** に示す．

構成例 1 は，復号された平文データが，FPGA か

ら外部の MPEG 伸張回路へ出力されている点で安全性は劣るが，ソフトウェア的な攻撃に対しては一定の強度を保ちつつ，比較的小規模の FPGA に実装できる．そのため，小型化に特化したポータブルプレイヤへの応用に向いている．

構成例 2 は，平文データの露出を防止するとともに，CSC を小型化することで通信コストを抑制可能であることから，携帯型プレイヤに適している．

構成例 3 は，構成例 2 の柔軟性と粒度を向上させ，よりリッチなコンテンツへの対応を可能にしている．ただし，CSC の規模は大きくなるため，通信コストは増大することから，ブロードバンドに対応した携帯型プレイヤへの応用に向いている．

構成例 4 は，ビデオ出力回路を内蔵することで，システム的な攻撃に対するコンテンツの安全性が高いことから，特に，映画等を大画面で視聴するための，据置き型 STB に向いている．

構成例 5 は，構成例 4 の柔軟性と粒度を向上させており，ブロードバンドに対応した据置き型 STB への応用に適している．

構成例 6 は，宅内における複数のユーザの視聴要求に対応できるコンテンツサーバ的な据置き型 STB に適している．

構成例 7 は，CSC の機能を動作制御とデータ入力インタフェースに限定することで，通信に対する負荷を最小化しており，放送型のペイパービューサービスを利用するための据置き型 STB に向いている．

8. おわりに

FPGA の動的部分再構成を用いたコンテンツ保護システムを提案した．このシステムは，コンテンツ固有回路（CSC）と端末固有回路（TBC）の 2 つの回路を FPGA 上で動的に結合し，その内部でコンテンツの復号や再生の処理を行うことを特徴としている．それによって，復号鍵や平文コンテンツに対するソフトウェア的なアクセスを遮断し，ウィルス等の攻撃に強いコンテンツ保護システムを構築できる．CSC と TBC の回路的な結合条件を端末ごとに変えることで，認証の手段を増やし，ロジック設計の推測を困難にするとともに，CSC やコンテンツの配信データが盗聴や複製によって流出したとしても，他の端末で利用されることを防ぐことができる．広帯域ネットワークを経由してリッチコンテンツを配信するサービスの再生用端末に適用すれば，CSC をコンテンツごとにカスタマイズすることで，コンテンツに適した復号・伸張処理が可能になるとともに，年々急速に進歩する著作権侵害技術に対抗する保護メカニズムを，端末の出荷後にも継続的に提供することができる．

本稿では，こうした CSC-TBC の結合メカニズムによるコンテンツ保護の基本コンセプトを実証するプロトタイプシステムを試作し，動作を検証した．開発環境としては，レクセオン・テクノロジー社の FPGA 開発用ボード REX2（REconfigurable EXperimental equipment 2）を使用し，ザイリンクス社の Virtex-II Pro における部分書き換え機能を用いてシステムを実装した．CSC の回路情報は暗号化された状態で配信され，TBC がこれを復号し，FPGA の再構成機能を用いて CSC を構築した．CSC と TBC の組合せが正しければ，両者は回路的に結合し，対応するコンテンツを再生できることを確認した．

今後の課題としては，CSC の認証機能を強化する，チャレンジレスポンス方式等のメカニズムの導入，サイドチャネル攻撃を考慮した回路構成技術の開発があげられる．

謝辞 日頃ご指導いただく KDDI 研究所秋葉所長，松本取締役，長谷川執行役員，産業技術総合研究所大蒔コーディネータ，坂上情報技術研究部門長，坂根主任研究員に感謝いたします．

参考文献

1) Whittaker, J.A. and Howard, M.: Computer Security, *IEEE mag. Security & Privacy*, Vol.2, No.5, pp.68–71 (2004).
2) 横山浩之，戸田賢二：FPGA を用いたコンテンツ保護システムの開発，信学技報，CPSY2004-114，pp.55–60 (2005).
3) Yokoyama, H. and Toda, K.: FPGA-Based Content Protection System for Embedded Consumer Electronics, *Proc. RTCSA 2005*, pp.502–507 (2005).
4) Hori, Y., Yokoyama, H. and Toda, K.: Secure Content Distribution System based on Run-Time Partial Hardware Reconfiguration, *Proc. FPL 2006*, pp.637–640 (2006).
5) 横山浩之，堀 洋平，戸田賢二：FPGA の部分書換方式を用いたコンテンツ保護システムの検討，信学技報，RECONF2006-34, pp.43–48 (2006).
6) White, S. and Comerford, L.: ABYSS: A trusted architecture for software protection, *IEEE Symp. Security and Privacy*, pp.38–51 (1987).
7) White, S., Weingart, W., Arnold, W. and Palmer, E.: Introduction to the Citadel architecture: Security in physically exposed environments, Distributed Security Systems Group, IBM Thomas J. Watson Research Center,

Tech. Rep. (1991).
8) Tygar, D. and Yee, B.: Dyad: A system for using physically secure coprocessors, Dept. Comput. Sci., Carnegie Mellon Univ., CMUCS-91-140R (1991).
9) Suh, G.E., O'Donnell, C.W. and Devadas, S.: AEGIS: A single-chip secure processor, *Inf. Security Tech. Rep.*, Elsevier, Vol.10, pp.63–73 (2005).
10) Zambreno, J., Honbo, D., Choudhary, A., Simha, R. and Narahari, B.: High-performance software protection using reconfigurable architectures, *Proc. IEEE*, Vol.94, No.2, pp.419–431 (2006).
11) Rouvroy, G., Standaert, F.-X., Lefebvre, F., Quisquater, J.-J., Macq, B. and Legat, J.-D.: Reconfigurable Hardware Solutions for the Digital Rights Management of Digital Cinema, *ACM Workshop on Digital Rights Management* (2004).
12) Trusted Computing Group (TCG). https://www.trustedcomputinggroup.org/home/
13) Ripley, M., Traw, C., Balogh, S. and Reed, M.: Content Protection in the Digital Home, *Intel Tech. J.*, Vol.6, Issue 4, pp.49–56 (2002).
14) Popescu, B.C., Crispo, B., Tanenbaum, A.S. and Kamperman, F.L.A.J.: A DRM Security Architecture for Home Networks, *ACM Workshop on Digital Rights Management* (2004).
15) 4C Entity: Content Protection for Recordable Media (CPRM) Specification. http://www.4centity.com/
16) Digital Content Protection, LLC: High-Bandwidth Digital Content Protection (HDCP) Specification. http://www.digital-cp.com/home/
17) Digital Transmission Licensing Administrator: Digital Transmission Content Protection (DTCP) Specification. http://www.dtcp.com/
18) High Definition Multimedia Interface (HDMI). http://www.hdmi.org/
19) U. S. Department of Commerce/National Institute of Standards and Technology: Security Requirements for Cryptographic Modules, FIPS PUB 140-2 (2001).
20) Anderson, R., Bond, M., Anderson, R., Bond, M., Clulow, J. and Skorobogatov, S.: Cryptographic Processors — A Survey, *Proc. IEEE*, Vol.94, No.2, pp.357–369 (2006).
21) U. S. Department of Commerce/National Institute of Standards and Technology: Data Encryption Standard (DES), FIPS PUB 46-3 (1999).
22) ANSI X9.52-1998.
23) U. S. Department of Commerce/National Institute of Standards and Technology: Announcing the Advanced Encryption Standard (AES), FIPS PUB 197 (2001).
24) Rouvroy, G., Standaert, F.-X., Quisquater, J.-J. and Legat, J.-D.: Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael Very Well Suited for Small Embedded Applications, *Proc. ITCC 2004*, Vol.2, pp.583–587 (2004).
25) Rivest, R., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
26) Xilinx: Two Flows for Partial Reconfiguration: Module Based or Difference Based, XAPP290 (v1.2) (2004).
27) Xilinx: Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet. http://www.xilinx.com/
28) Xilinx: Virtex-II Pro and Virtex-II Pro X FPGA User Guide. http://www.xilinx.com/
29) Xilinx: Development System Reference Guide (for ISE 8.1i) (2005).
30) Xilinx: PlanAhead User Guide Release 8.2. http://www.xilinx.com/

(平成 18 年 11 月 27 日受付)
(平成 19 年 6 月 5 日採録)

横山 浩之（正会員）

1992 年京都大学工学部電子工学科卒業．1994 年同大学院修士課程修了．同年国際電信電話（株）（現 KDDI（株））入社．以来，研究所にて，ATM 網，移動通信網，IP 網，光パケット網の性能評価・設計に関する研究に従事．2004 年より，組み込み機器のプラットフォーム構築に関する研究に従事．2000 年（社）電子通信学会学術奨励賞受賞．電子情報通信学会会員．博士（工学）．

堀　洋平（正会員）

1999 年筑波大学第三学群工学システム学類卒業．2004 年同大学院博士課程修了．同年（独）産業技術総合研究所情報処理研究部門（現，情報技術研究部門）特別研究員．多目的映像表示装置，コンテンツ保護システム等の研究開発を行う．現在，FPGA の部分再構成を利用したリコンフィギャラブルシステム，LSI の耐タンパ性評価に関する研究に従事．電子情報通信学会会員．博士（工学）．

戸田　賢二（正会員）

1982 年慶應義塾大学大学院工学研究科修士課程修了．同年電子技術総合研究所（現（独）産業技術総合研究所）入所．以来，並列コンピュータのアーキテクチャの研究に従事し，記号処理用データ駆動計算機や実時間処理用並列計算機の開発を行った．近年は，組み込み応用をターゲットとし，FPGA による開発環境の整備とともに，高速ネットワークセキュリティ機器や高機能映像表示装置等の実用化研究を推進中．産総研情報技術研究部門実時間組込システム研究班長．電子情報通信学会会員．