報道発表

- **カオス暗号チップを開発し、デジタルハイビジョン映像のリアルタイム暗号化通信に世界で初めて成功**
- **平成15年4月15日**

独立行政法人通信総合研究所（理事長：飯田尚志、CRL）は、デジタルハイビジョン映像のリアルタイムの暗号化、伝送及び復号化に世界で初めて成功しました。本通信実験の暗号アルゴリズムは、カオス理論を基に設計されたハードウェア、ソフトウェア両プラットフォームで、高速のストリーム暗号「VSC」（ブイ・エス・シー:Vector Stream Cipher）です。

本実験で実証された暗号化処理速度は１秒間に14.85Gbitの暗号化できるスピードで伝送、復号化を含む暗号通信の実験としては世界最高速となります

＜背景＞
映像など各種のデジタルコンテンツが、品質の劣化なしにネットワーク上で広範に配信・流通するようになれば新たな市場が創出され、その経済的インパクトは非常に大きいものになると言われています。そのデジタルコンテンツ配信・流通において緊急な課題が、著作権や医療データ等の個人のプライバシーを保護するための暗号化技術の確立です。

＜概要＞
CRLでは、カオス理論に基づく新しい暗号処理アルゴリズム「VSC」（ブイ・エス・シー:Vector Stream Cipher）を開発し、取得した特許を積極的に技術移転してきました（実施許諾先は3社）。
平成１３年度からは、理事長ファンド・プレベンチャー制度の「カオス暗号チップの研究開発」において、デジタルコンテンツ流通・配信を支えるリアルタイムで動作するセキュリティ技術を確立するため「VSC」のLSIチップ化による高速暗号プロセッサーを開発してきました。

今回、処理速度の高速化のための改良をおこない、伝送、復号化を含む暗号通信の実験としては世界最高速となる１秒間に14.85Gbitの暗号化処理速度を実現しました。デジタルハイビジョン映像のリアルタイムの暗号化、伝送及び復号化の実証に世界で初めて成功したものです。

＜今後の展開＞
本高速ストリーム暗号「VSC」の普及を目指す「VSCコンソーシアム」を８月に設立し（CRL内）、産・学・官の連携で、大容量データの高速リアルタイム暗号化・復号化・伝送システムの実用化のための検証を更に行います。医療データ等の大容量高精細画像や動画などのデジタルコンテンツをリアルタイム暗号化することによる配信・流通におけるセキュリティ技術を確立します。

＜連絡先＞
超高速フォトニックネットワークグループ
梅野　健　　TEL 042-327-6399

<補足資料>

本システムの全体像と暗号化／復号化ユニット部を図1に示します。
このシステムでは、ハイビジョンカメラから入力されたデジタルハイビジョン映像であるHD-SDI信号（SMTE-292M）を暗号化ユニットに送り、それを10本のHD-SDI信号に並列化し、カオス暗号「VSC」を用いて暗号化を行います。

暗号化されたデータは Rocket I/O にて復号化ユニットに転送され、復号化された結果をモニタで見ることができます。暗号化／復号化ユニットはそれぞれ2枚のボードからなっており、上部のボードでハイビジョンデータの変換を行ない、下部のボード（Xilinx 社製 ML321ボード）にて暗号化／復号化処理と、Rocket I/O を用いたデータ転送を行います。暗号化ユニットでは、ハイビジョンカメラから入力されたデジタルハイビジョン映像が上部のボードでデータ変換され下部のボードに転送されます。下部のボードではデジタルハイビジョンデータの映像部分を暗号化し、Rocket I/O にて復号ユニットの下部のボードに送られます。

復号ユニットでは、下部のボードで送られてきたデータの復号化を行ない、上部のボードにデータを転送し、上部のボードでハイビジョン映像信号に変換を行ないモニタから出力します。

暗号化／復号化の処理スピードは 14.85 Gbps で、Rocket I/O での転送は、23.76 Gbps となります。Rocket I/O での転送レートが増加するのは、暗号化している画像データ以外に sync 信号や Rocket I/O で通信するためのヘッダなどが付加されるためです。

図1－1：全体システム

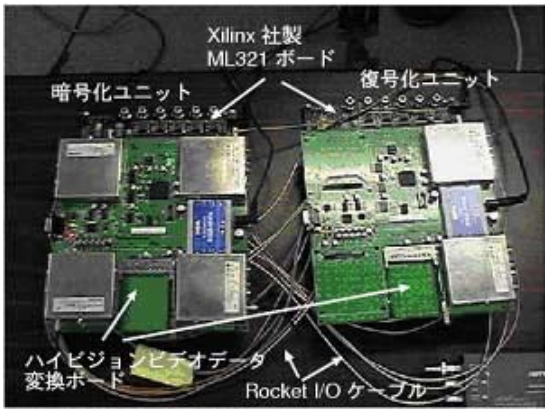

図1－2：暗号化・復号化ボードの概要

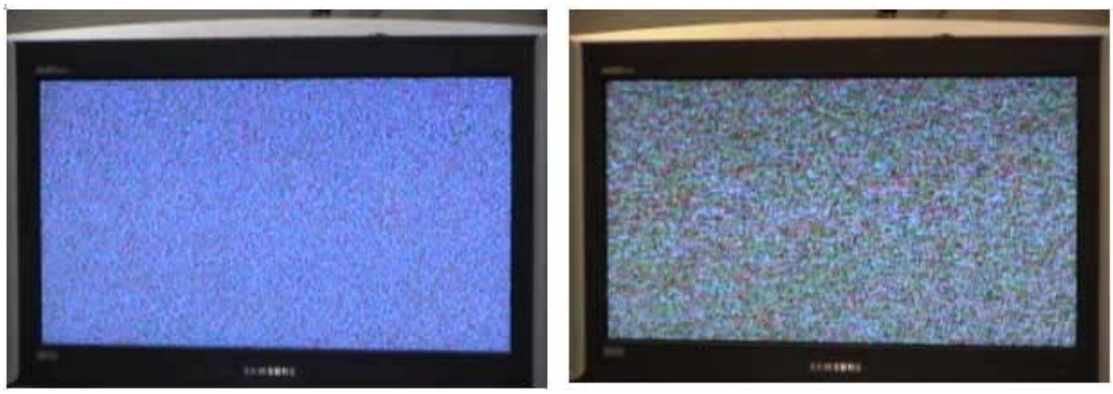

図2-1:暗号化されたデジタルハイビジョン映像(左)と通常のNTSCテレビ映像(右)

図2-2:復号化されたデジタルハイビジョン映像(左)と通常のNTSC映像(右)

＜用語解説＞

HD-SDI:
High-Definition Television- Serial Digital Interfaceの略。
BTA S-004B及びSMPTE292Mで規定されているHDTV用の1.485Gbit/secのシリアルデジタルインターフェース

カオス:
一見ランダムに見えるが背後に規則がある現象。カオスを乱数生成器として用いるカオス暗号は、今までもソフトウェアにより実現するものがあったが、今回開発したカオス暗号チップは、カオス暗号アルゴリズム「VSC」をLSIに実装したことが他のカオス暗号と異なる特徴となっている。

VSC:
Vector Stream Cipherの略。Stream Cipherは秘密鍵暗号の一種であるストリーム暗号の略で、逐次的に処理する暗号。そのストリーム暗号のプロセスを並列処理することにより、暗号強度と暗号スピードを高める新しい秘密鍵暗号アルゴリズムが、VSCである。
VSCを用いたセキュリティ製品としてVSC特許(特許第3030341号)のライセンス許諾先の1社であるジャパン・インフォメーション・テクノロジー社と共同開発したデータベース暗号化　ソフトウェア「eCipherGate」がある。

VSCの基本特許のより詳細な情報は、以下のCRL開放特許ウェブサイトから取得できる。
http://www2.crl.go.jp/kk/e416/tokkyo/koukai/detail/411.htm