様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年 ５月 ３１日現在

機関番号：３７１０２
研究種目：挑戦的萌芽研究
研究期間：2009～2011
課題番号：２１６５６０９９
研究課題名（和文） 暗号領域における信号処理 －暗号化された信号を処理する技術の開発－
研究課題名（英文） Signal processing in the encrypted domain - Development of a new technique for secure manipulation of signals -
研究代表者
宮崎 明雄（MIYAZAKI AKIO）
九州産業大学・情報科学部・教授
研究者番号：70192763

研究成果の概要（和文）：本研究では、暗号により秘匿化された信号を復号することなく、暗号領域において様々な情報を担う信号を処理し活用するための基礎技術の構築を行った。まず、信号処理の実数演算を有理数演算、更に整数演算で近似する方法を与えた。これにより信号領域の積和演算が暗号領域のべき積演算に対応付けられ、加法的準同型性をもつ暗号の適用が可能になった。次に、準同型性暗号を用いて画像信号の暗号領域における認証システムを提案した。研究成果は情報漏えい防止やプライバシー保護に関する諸問題への応用が可能である。

研究成果の概要（英文）：We have established the fundamental techniques for computing with signals that are encrypted or otherwise hidden often referred to as signal processing in the encrypted domain. We have first presented a method of approximate conversion from signal processing operations with real numbers to those with rational numbers such as integers and fractions. It follows from this that we can transform multiplications and summations in the signal processing domain into power operations and multiplications in the encrypted domain, and implement signal processing in the encrypted domain with an additive homomorphic encryption. Using this method, we have proposed an image authentication system in the encrypted domain. The results are considered to play an important role in real-world applications in which cryptography meets signal processing.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,000,000	0	1,000,000
２０１０年度	1,000,000	0	1,000,000
２０１１年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	300,000	3,300,000

研究分野：情報セキュリティ、信号処理、画像処理
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：情報通信工学、情報セキュリティ、信号処理、画像処理、暗号・認証、公開鍵暗号、準同型性暗号、電子透かし

１．研究開始当初の背景

近年の半導体・システム LSI 技術の進歩とコンピュータネットワークの普及により、音声・音響・画像情報や文字・図形情報がディジタル化されマルチメディア情報として、CD・DVD や光・磁気ディスクサーバに記録蓄積され、世界中からコンピュータネットワ

ークを通してこれらのマルチメディア情報に容易にアクセス・コピーできるようになってきている。同時に、そうしたマルチメディア情報を不正に利用する犯罪も目立つようになってきている。このため著作権保護やコピー制御を目的として暗号でマルチメディア情報を保護することが行われている。しかしながら、暗号化された情報も一旦復号されると不正利用に対しては無力である。そこで、研究代表者を含め多くの研究者が約 15 年前から電子透かし（Digital Watermark）の研究を行っているが、電子透かしはそうした不正利用を抑止する効果しかないのが現状である。また、数学的（理論的）に安全な電子透かし（情報信号に対して攻撃や処理を行っても電子透かしが壊れないこと）を作るのは困難なようである。そこで、研究代表者は本研究のような情報を担う信号を秘匿したまま処理するという研究の必要性を痛感している。

情報を秘匿したまま活用する技術として、暗号理論・暗号技術の分野では、ゼロ知識対話証明や秘密分散法などが知られており、電子投票や電子入札、電子マネーなどに応用されている。他方、信号処理の分野では指紋認証などの生体認証に応用されている。しかしながら、信号領域での各種演算処理を暗号領域で行うような技術は構築されていない。その主な理由は、信号処理の演算が実数・複素数演算であるのに対し、暗号処理の演算が整数・剰余演算であることによると思われる。本研究ではこのような点を考慮して、信号領域から暗号領域への変換と暗号領域における信号処理に関する理論の提案を行うとともに、情報信号の保護が必要とされる分野への応用を考えるものである。

２．研究の目的

情報漏えいやプライバシー保護の観点からは、音や画像など様々な情報を担った信号を何らかの形で秘匿することが望ましい。しかしながら、情報を担う信号は活用するために存在するものである。活用するためには秘匿された信号を復元しなければならないが、そのタイミングが重要である。そこで情報漏えいが発生すれば信号を秘匿する意味がなくなってしまう。したがって、暗号化された信号を復号することなく、暗号領域において様々な情報を担う信号を活用するという方向性の研究は今後益々重要になってくると思われる。このため、本研究では、暗号化された信号を復号することなく処理するための基礎技術について検討を行い、暗号領域における信号処理技術を構築する。

本研究により信号領域から暗号領域への新しい変換・処理技術が得られれば、この技術を無線通信や画像処理の分野へ直ちに応用することが可能になる。例えば、医療画像情報を無線伝送し、診断結果を返信するような場合など、無線通信路で画像情報を伝送し、受信側で何らかの処理をして活用する場合、セキュリティの問題は重要である。本研究の成果はこのような分野におけるセキュリティの問題に適用できると考えられる。

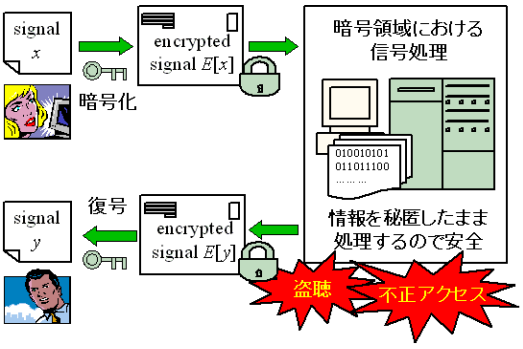

図１：暗号領域における信号処理

３．研究の方法

信号処理の基本演算は、積和演算、たたみ込み演算、線形変換などの演算であり、非線形演算などの信号処理演算は基本演算で近似することができる。また、信号処理の中には、数論変換やリフティングフィルタバンクなど、整数型の信号を直接取り扱う演算処理がある。

他方、暗号処理の基本演算は整数論をベースとしている。本研究では、暗号の中でも特に加法性の準同型性を有する暗号（加法的準同型性暗号）に着目する。加法的準同型性暗号は次の性質をもっている。

平文 m_1, m_2 の暗号文をそれぞれ $E[m_1]$, $E[m_2]$ とするとき、

$$E[m_1 + m_2] = E[m_1] \times E[m_2]$$

が成り立つ。ここで $E[\bullet]$ は暗号化を表す演算子である。この性質から、平文 $m_1 + m_2$ の暗号文 $E[m_1 + m_2]$ を、$E[m_1]$, $E[m_2]$ を復号することなく（情報を秘匿したまま）直接計算することができる。また、平文 m と定数 a に対して

$$E[am] = \{E[m]\}^a$$

も成り立つ。

信号領域の演算から暗号領域の演算への変換は準同型性暗号を用いることにより可能となる。例えば、準同型性暗号を用いると、信号 x_k の積和演算

$$y = \sum_k a_k x_k$$

の暗号文 $E[y]$ は

$$E[y] = E\left[\sum_k a_k x_k\right] = \prod_k \{E[x_k]\}^{a_k}$$

と変換でき、信号 x_k の暗号文 $E[x_k]$ から直接計算することができる。

しかしながら、信号処理の演算は一般に実数・複素数演算であるのに対し、暗号の演算は整数・剰余演算である。信号領域の演算を暗号領域の演算に変換するためには、信号処理の実数・複素数演算を整数演算に変換する、あるいは近似する必要がある。このような変換・処理の理論について考察し、暗号領域における信号処技術としてまとめることを目的とする本研究は斬新性・チャレンジ性を有していると思われる。

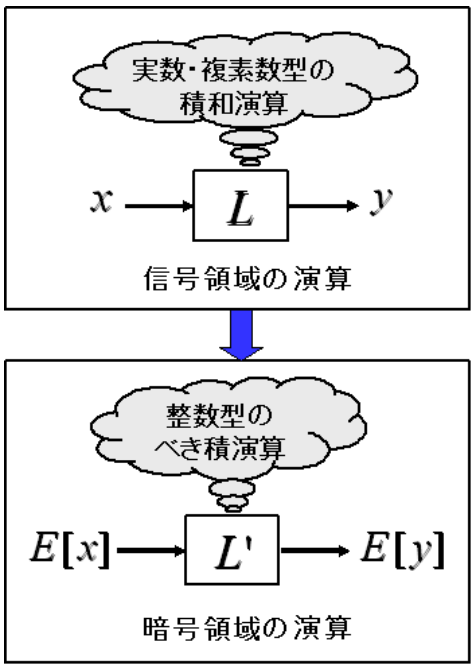

図２：信号領域から暗号領域への変換

研究目的を達成するための研究計画・方法は以下の通りである。本研究を理論開発面から見ると次の要素研究に分割され、実行される。研究期間は３年間である。

(1) 信号処理の基本演算（積和演算、たたみ込み演算、線形変換など）を分類整理する。また、基本演算以外の信号処理演算（非線形演算など）を基本演算で近似する手法について調査・研究する。
(2) 暗号、特に準同型性を有する暗号（準同型性暗号）について調査し分類整理する。また、準同型性暗号を用いた応用事例について調査・研究する。
(3) 信号処理の中には、数論変換やリフティングフィルタバンクなど、整数型の信号を直接取り扱う演算処理がある。このような演算を暗号領域の演算に変換するための手法について調査・研究する。
(4) 信号処理の演算は一般に実数・複素数演算であるのに対し、暗号の演算は整数・剰余演算である。信号領域の演算を暗号領域の演算に変換するためには、信号処理の実数・複素数演算を整数演算に変換する、あるいは近似する必要がある。このような変換・近似の手法について調査・研究する。
(5) 信号処理の整数型・実数型・複素数型演算を暗号領域の整数演算に変換する、あるいは近似するための方法を開発し、実装する。また、暗号領域における信号処理の精度に関する検討も行う。
(6) 暗号領域における信号処理の実験的検証を行う。画像信号を対象とした実験的検証を行い、その結果をもとに提案手法の改良等を行う。
(7) 上記の理論を無線通信や画像処理の分野へ応用する。高精細画像を無線伝送し、受信側で何らかの処理をしてその結果を活用する場合、セキュリティの問題は重要である。このようなハイビジョン画像のセキュア・ワイヤレス伝送問題に対して、本研究の成果が適用できるかどうか検討する。

４．研究成果

本研究の実施計画に対する研究成果を年度ごとにまとめる。

【平成 21 年度】

(1) 信号処理の基本演算としてコンボリューション（たたみ込み）演算、その逆問題としてデコンボリューション演算がある。ここでは、情報通信や画像処理の分野で現れるブラインド・デコンボリューションの問題について検討を行い、信号や画像の歪みモデルが未知ではあるが、その平均や共分散などの統計的性質が既知あるいは推定可能な場合について、EM アルゴリズムを用いた解決法を提案した。このアプローチにより電子透かし検出システムの補正アルゴリズムを与えた。
(2) 暗号領域における信号処理において重要な役割を担う準同型性暗号について調査し分類整理を行った。特に、乗法性の準同型性をもつ RSA 暗号と加法性の準同型性をもつ Paillier 暗号について調査・研究を行った。また、RSA 暗号と Paillier 暗号について、鍵生成と暗号化、復号のアルゴリズムをソフトウェアで実装し、動作確認および準同型性の確認を行った。
(3) RSA 暗号の乗法的準同型性を利用して、暗号領域において画像の注目領域を抽出するという応用事例を示した。Paillier 暗号の加法的準同型性を利用して、暗号領域おいてデータの統計処理をするという

応用事例を示した。また、電子透かし入り画像の準同型性暗号による暗号化（スクランブル）と、暗号領域における電子透かしの検出について検討を開始した。

(4) 暗号領域における信号処理の実験的検証を行うため、画像伝送システムおよび無線伝送システムの環境整備を開始した。

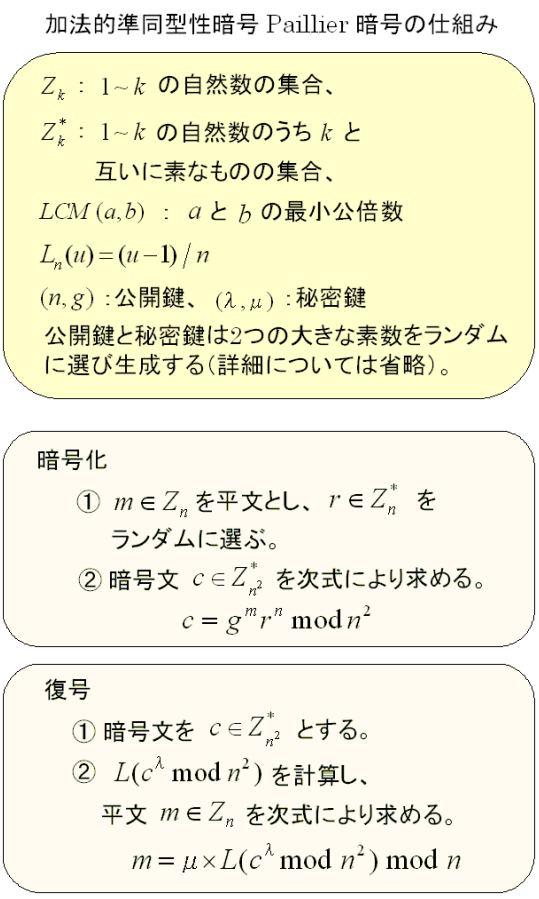

図３：Paillier 暗号の仕組み

【平成 22 年度】

(1) 信号領域の実数演算を暗号領域の整数・剰余演算に変換するためには、信号処理の実数演算を整数演算に変換または近似する必要がある。下記(4)との関連で信号の内積・ノルム演算に対して実数型から整数型への変換手法を与えた。

(2) 暗号領域における信号処理において重要な役割を担う準同型性暗号の調査・研究を継続して行った。特に、加法的準同型性暗号 Paillier 暗号について研究を行った。前年度開発した Paillier 暗号の鍵生成と暗号化、復号のプログラムについて、暗号の安全性を高めるために、鍵の長さ（素数の桁数）をより大きくするなどプログラムの改良を行い、これをソフトウェアで実装し、動作確認および準同型性の確認を行った。

(3) 暗号領域での検出が可能な画像への電子透かしの埋め込み法について検討した。可逆コンポーネント変換と整数型ウェーブレット変換により、カラー画像をウェーブレット係数（整数値）に変換する。複数個のウェーブレット係数の積和演算で透かしの検出が行えるように透かしの埋め込み処理を行う。これにより準同型性暗号の適用が可能となる。透かし情報の検出精度と透かし入り画像の画質を数値実験により評価した。

(4) 画像情報を暗号化し、暗号領域でその識別・判定を行うシステムについて研究した。識別・判定では類似度法（内積・ノルム計算）を用いた。Paillier 暗号の加法的準同型性により暗号化されたまま画像認証を行い、チャレンジ＆レスポンス認証を応用して情報が漏洩しても安全性を保つことができるシステムを提案した。

(5) 暗号領域における信号処理の実験的検証を行うため、Paillier 暗号による JPEG2000 動画像の認証システムを構築し、その環境整備を行った。

【平成 23 年度】

(1) 信号処理の基本演算は積和演算で、一般に実数演算であるのに対し、暗号は整数演算である。信号領域の実数演算を有理数演算で近似し、積和演算の分子と分母を別々に計算することにより、整数演算に変換するための手法を与えた。これにより、信号領域の積和演算を暗号領域のべき積演算に対応付けることができ、加法的準同型性をもつ暗号の適用が可能になった。

(2) 加法的準同型性暗号 Paillier 暗号に関して、前年度開発した鍵生成と暗号化、復号のプログラムについて引き続き検討した。暗号の安全性を更に高めるため、Java 言語の BigInteger 型を用いて鍵の長さ（素数の桁数）をより大きくするなどプログラムの改良を行い、これをソフトウェアで実装し、動作確認および準同型性の確認を行った。

(3) 暗号領域での検出が可能な画像への電子透かしの埋め込み法について引き続き検討した。提案手法で作られた透かし入り画像に対し、上記(2)で改良した Paillier 暗号プログラムを用いて暗号化し、暗号領域において透かし情報が検出できることを確認した。

(4) これまでに得られた研究成果を応用し、暗号領域における信号処理の実験的検証を行った。特に、画像伝送システムおよび無線伝送システムを構築し、Paillier 暗号による JPEG2000 画像の暗号領域における認証システムを提案した。その結果を論文 Image Transmission using

Encryption Domain Authentication for Mesh Network としてまとめ、国際会議 2011 International Workshop on Smart Info-Media Systems in Asia で発表した。

本研究で得られた信号領域から暗号領域への変換および暗号領域における信号処理に関する新しい手法など、これらの成果は無線通信や画像処理の分野へ直ちに応用することが可能になる。例えば、

(1) 医療画像情報を無線伝送し、受信側で何らかの処理を行い、診断結果などを返信する場合
(2) 指紋などの生体情報を無線伝送し、受信側で識別・判定を行い、その結果を返信する場合
(3) デジタルシネマのような高精細ディジタル画像を無線伝送し、受信側でユーザ認証などの処理を行って再生する場合

など、情報を担った信号を無線伝送し、受信側で何らかの処理をして活用する場合、セキュリティの問題（セキュア・ワイヤレス伝送問題）は重要である。本研究の成果はこのような分野におけるセキュリティ問題の解決に適用できると考えられる。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 18 件）

① Koji Inoue and Yoshimitsu Kuroki, “On Sparse Representation for Face Recognition under Illumination Change,” Proc. of the 2012 International Workshop on Advanced Image Technology, Vol.1, pp.662-667, 2012 年 1 月，査読有.
② Shoma Eguchi, Koji Inoue, Yoshimitsu Kuroki, Masayuki Kurosaki, Yuhei Nagao, and Hiroshi Ochi, “On Parallel 2D-DWT of JPEG 2000 conformed to Digital Cinema Initiatives using GPGPU,” Proc. of the 2012 International Workshop on Advanced Image Technology, pp.668-671, 2012 年 1 月，査読有.
③ Muneaki MATSUO, Masayuki KUROSAKI, Akio MIYAZAKI, and Hiroshi OCHI, “Image Transmission using Encryption Domain Authentication for Mesh Network,” Proc. of the 2011 International Workshop on Smart Info-Media Systems in Asia, Vol.1, pp.57-60, 2011 年 11 月，査読有.
④ Masayuki KUROSAKI, Masateru MATSUO, Yoshimatsu KUROKI, Yuhei NAGAO, Baiko Sai, and Hiroshi OCHI, “A CUDA Implementation of DWT for JPEG 2000 Codec,” IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E94-A, No.11, pp.2358-2360, 2011 年 11 月，査読有.
⑤ Masateru Matsuo, Ryo ito, Masayuki Kurosaki, Baiko Sai, Yoshimitsu Kuroki, Akio Miyazaki, and Hiroshi Ochi, “Wireless Transmission of JPEG 2000 Compressed Video,” Proc. of the 13th International Conference of Advanced Communication Technology, CD-ROM, 4 pages, 2011 年 2 月，査読有.
⑥ Masateru Matsuo, Msasyuki Kurosaki, Yuhei Nagao, Sai Baiko, Yoshimitsu Kuroki, Akio Miyazaki, and Hiroshi Ochi, “HDTV over MIMO Wireless Transmission System,” Proc. of the 2011 IEEE Consumer Communications and Networking Conference, CD-ROM, 4 pages, 2011 年 1 月，査読有.
⑦ Nobuhiro FUNATSU and Yoshimitsu KUROKI, “Parallel Processing on PCA-L1,” Proc. of the 2010 Workshop on Picture Coding and Image Processing, pp.107-108, 2010 年 12 月，査読有.
⑧ Nobuhiro FUNATSU and Yoshimitsu KUROKI, “Fast Parallel Processing Using GPU in Computing L1-PCA Bases,” Proc. of TENCON2010 - 2010 IEEE Region 10 Conference, Vol.1, pp.2087-2090, 2010 年 11 月，査読有.
⑨ Yoshimitsu Kuroki, Masateru Matsuo, Yuhie Nagao, Baiko Sai, Akio Miyazaki, Masayuki Kurosaki, and Hiroshi Ochi, “A CUDA Implementation of JPEG 2000 Codec for 4K Digital Cinema Wireless Transmission System,” Proc. of the 2010 International Workshop on Smart Info-Media Systems in Asia, CD-ROM, 4 pages, 2010 年 9 月，査読有.
⑩ Masayuki Kurosaki, Masateru Matsuo, Yoshimitsu Kuroki, Akio Miyazaki, and Hiroshi Ochi, “HDTV Wireless Streaming Using IEEE802.11ac 4x5 MIMO WLAN System,” Proc. of the 2010 International Workshop on Information Communication Technology, CD-ROM, 4 pages, 2010 年 8 月，査読有.
⑪ Masayuki KUROSAKI, Masateru MATSUO, Yuya HIRATA, Hiroshi OCHI, Wahyul Amien Syafei, Yuhei NAGAO, Baiko SAI, Akio MIYAZAKI, and Yoshimitsu KUROKI, “4K Digital Cinema Transmission Over 1.2Gbps Wireless LAN System,” Proc. of

the 7th Annual IEEE Consumer Communications and Networking Conference, CD-ROM, 4 pages, 2010年1月, 査読有.

⑫ Nobuhiro Funatsu and Yoshimitsu Kuroki, “Fast Method of Principal Component Analysis based on L1-Norm Maximization Algorithm,” Proc. of the Asia Pacific Signal and Information Processing Association 2009 Annual Summit and Conference, Vol.1, pp.262-265, 2009年10月, 査読有.

⑬ Akio Miyazaki, “A Sequence Estimation Method based on EM Algorithm and Its Application to the Watermark Detection Problem,” Proc. of the Asia Pacific Signal and Information Processing Association 2009 Annual Summit and Conference, Vol.1, pp.410-413, 2009年10月, 査読有.

⑭ Yuta Kuboyama and Yoshimitsu Kuroki, “Fast Mode Decision for H.264/AVC on SATD Value,” Proc. of the Asia Pacific Signal and Information Processing Association 2009 Annual Summit and Conference, Vol.1, pp.461-464, 2009年10月, 査読有.

⑮ Wahyul Amien Syafei, Yuhei Nagao, Masayuki Kurosaki, Baiko Sai, and Hiroshi Ochi, “A 1.2 GBPS Wireless LAN System for 4K Digital Cinema Transmission,” Proc. of the Asia Pacific Signal and Information Processing Association 2009 Annual Summit and Conference, Vol.1, pp. 785-790, 2009年10月, 査読有.

⑯ Yuta Higuchi and Yoshimitsu Kuroki, “Arbitrarily Shaped Transform Coding based on Modification of Pixels in Shapes,” Proc. of the Asia Pacific Signal and Information Processing Association 2009 Annual Summit and Conference, Vol.1, pp. 833-836, 2009年10月, 査読有.

⑰ Yuya HIRATA, Masateru MATSUO, Masayuki KUROSAKI, Wahyul Amien Syafei, Baiko SAI, Yuhei NAGAO, Hiroshi OCHI, Yoshimitsu KUROKI, and Akio MIYAZAKI, “Digital Cinema Wireless Transmission and Its Windows Application,” Proc. of the 2009 International Symposium on Communications and Information Technology, CD-ROM, 4 pages, 2009年9月, 査読有.

⑱ Akio Miyazaki, “A Solution to the Watermark Detection Problem Based on Bayesian Estimation and EM Algorithm,” Proc. of the 17th European Signal Processing Conference, Vol.1, pp.1789-1793, 2009年8月, 査読有.

〔学会発表〕(計6件)

① 黒崎正行, 伊東亮, 松尾宗明, 宮岡佑弥, 井上昂治, 江口翔馬, 尾知博, 黒木祥光, 宮崎明雄, “暗号領域での認証を用いたJPEG 2000画像無線伝送システム,” 電子情報通信学会2012年総合大会, 2012年3月23日, 岡山大学 (岡山市).

② 廣川真梨子, 黒木祥光, “基底の選別とグラムシュミットの直交化を用いたPCA-L1の高速化,” 電子情報通信学会 第26回信号処理シンポジウム, 2011年11月16日, 札幌コンベンションセンター (札幌市).

③ 松尾正輝, 井上昂治, 黒崎正行, 黒木祥光, 斉培恒、尾知博, “4Kデジタルシネマ無線伝送システムのための JPEG 2000 並列化,” 画像電子学会 第 255 回研究会, 2011年3月3日, 鹿児島大学(鹿児島市).

④ 平田雄也, 黒崎正行, 宮崎明雄, 尾知博, “JPEG2000動画像のPaillier認証システムに関する研究,” 画像電子学会 第 255 回研究会, 2011年3月3日, 鹿児島大学 (鹿児島市).

⑤ 松尾正輝, 平田雄也, Wahyul Amien Syafei, 黒崎正行, 黒木祥光, 宮崎明雄, 斉培恒, 尾知博, “4Kデジタルシネマの1.2Gbps無線LAN伝送システム,” 電子情報通信学会スマートインフォメディアシステム研究会, 2009年9月24日, 広島大学(広島市).

⑥ 江藤美帆, 冨永康子, 松尾正輝, 平田雄也, Wahyul Amien Syafei, 黒崎正行, 斉培恒, 黒木祥光, 宮崎明雄, 尾知博, “デジタルシネマ画像の無線伝送システム,” 第11回DSPS教育者会議, 2009年9月11日, 東京工業大学 (東京都).

６．研究組織

(1)研究代表者
宮崎 明雄 (MIYAZAKI AKIO)
九州産業大学・情報科学部・教授
研究者番号：70192763

(2)研究分担者
黒木 祥光 (KUROKI YOSHIMITSU)
久留米工業高等専門学校・
制御情報工学科・准教授
研究者番号：60290847
黒崎 正行 (KUROSAKI MASAYUKI)
九州工業大学・大学院情報工学研究院・
准教授
研究者番号：80404094

(3)連携研究者
なし