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

2006－ＳＬＤＭ－126（１）
2006／10／26

集積回路内 IP コア間の暗号化通信方式

早川 雅文† 中村 次男†† 笠原 宏† 冬爪 成人† 田中 照夫†††

† 東京電機大学情報環境学部 〒270-1382 千葉県印西市武西学園台 2-1200
†† 国際短期大学情報ネットワーク学科 〒165-0022 東京都中野区江古田 4-15-1
††† 東京電機大学工学部電気工学科 〒101-8457 東京都千代田区神田錦町 2-2

E-mail: † kasahara@itl.sie.dendai.ac.jp

あらまし 開発元の異なる多種多様な IP コアをひとつのチップ上に集積化するシステム LSI やシステム・オン・チップ(SoC)という超高集積回路時代に向けて，課題となっている IP コア間のインタフェースの標準化およびバス調停機構を含めた IP コア間の通信方式を提案する。ネットワーク・オン・チップにおける GALS の同期回路部分に関する通信方式で，IP コアとオン・チップ・バス間に通信制御機構を配置する。IP コアからの通信データを通信制御機構で暗号化し，バスに送出する。これによりバス上のデータを隠蔽するとともに IP コアの盗用防止を図る。

キーワード システム LSI，システム・オン・チップ，IP コア，モジュール化，ネットワーク・オン・チップ

A Cryptographic Communication Technique between IP Cores in ULSI

Masafumi HAYAKAWA† Tsugio NAKAMURA†† Hiroshi KASAHARA†
Narito FUYUTSUME† and Teruo TANAKA†††

† Department of Information Environment Engineering School of Information Environment, Tokyo Denki University
Muzaigakuendai 2-1200, Inzai-shi, chiba, 270-1382 Japan
†† Department of Information and Network, kokusai Junior College
egota 4-15-1, nakano-ku, Tokyo, 165-0022 Japan
††† Department of Electrical Engineering School of Engineering, Tokyo Denki University
kandanishikichou 2-2, chiyoda-ku, Tokyo, 101-8457 Japan
E-mail: † kasahara@itl.sie.dendai.ac.jp

Abstract The paper proposes a communication method between IP cores, including the standardization on the interface between IP cores, and the bus mediation mechanism aiming at the super high integration circuit age like system LSI and system on chip(SoC), that integrates various IP cores with a different development origin, on a single chip. The integrated communication controller is arranged for the communication control, on the ground that it is applied for the synchronous circuit part of GALS for the network on chip. The communication data from the IP core is encrypted by the integrated communication controller, and sent out to the bus. As a result, data on the bus is concealed and prevented from the IP core design plagiarizing.

Keyword system LSI, system on chip, intellectual property core, modularization, network on chip

1. まえがき

システム LSI，システム・オン・チップ(SoC)およびシステム・イン・パッケージ(SIP)といった超高集積回路技術によって，10 年以内に，数十から数百という回路ブロック（Intellectual Property Core：IP コア）が一つのチップ上に集積可能となると予測されている[1],[2]．この規模の集積化においては電源電圧と消費電力，IP コア間の同期化とインタフェースの標準化および通信方式など課題が存在する。各 IP コア間の接続は，従来のバス型ネットワークでは性能と電源の障害になることから，各 IP コア間を相互に接続するネットワーク・オン・チップ(NoC)の構想が報告されている。また，

このような大規模なチップの全回路ブロックを一つの機関で設計することは設計に要する時間やコストなどから困難である。これにはIPコアの再利用とその流通形態が重要性を増す。しかし，開発元の異なるIPコアの再利用にはインタフェースの標準化が不可欠であるが，各社それぞれ特定の技術を持って競合している現状を考慮すれば，その標準化は大変な問題である。この問題に対して多くの研究報告がなされており，1つは，各ノードに接続されたIPはルータを介してパケット方式で通信[1]，次に，各IPコア間の同期化に関しては，「大局的に非同期式/局所的に同期式（GALS）」[3],[4],[5]，そして，データを1クロックサイクルで転送可能な大きさに分割し，パケット方式を用いずルーティング情報は別の配線で並走させる[6]などがある。

これまで筆者らは，GALSの例を注目しており，IPコアをオブジェクト指向における1オブジェクトとしてとらえ，オブジェクト間で送受信されるメッセージとパラメータという非常に簡素なフォーマットのメッセージ通信を行うことによって，インタフェースの標準化を容易にする研究を行ってきた。IPコアとデータバスの間に通信の制御を行う機構(Access Control Unit: ACU)を配置(各IPコアにそれぞれのACU)することによりIPコアはそのACUとのメッセージ通信によって目的とするIPコアと通信を行う方法を提案するものである[7],[8]。ここでは，通信データの盗視によるデータ解析とIPコアの盗用に対し，暗号機構を内蔵し，IPコア間で送受信される通信データをすべて暗号化し通信データの隠蔽を行う方法を提案する。大規模なチップを設計するにあたり，開発元の異なるIPコアを使用する際に通信データを隠蔽し，各IPコアの盗用を防止することはシステムの信頼性向上のためにも不可欠である。

2. 暗号化通信の意義

1.で述べたようにNoCのような大規模なチップを一つの機関で設計することは非常に困難であり，流通する開発元の異なるIPコアを使用することが必要不可欠となる。開発元の異なるIPコアを使用するにあたり，IPコア間でデータ通信を行う際，通信データの盗視により通信データが解析され，目的とするIPコアが特定されて盗用されるということが懸念されている。

そこで，提案する通信機構に暗号機構を内蔵し，IPコア間で送受信される通信データをすべて暗号化し，通信データの隠蔽を図る。

通信機構に暗号機構を内蔵することで暗号機構の無い通信機構に比べ処理時間は長くなるが，通信データの隠蔽，盗用の防止を考慮することでIPコアの流通形態の安全性が向上し，データ漏洩を防止することができる。

3.で暗号機構が内蔵されていない通信機構，4.で暗号機構の内蔵された通信機構について述べる。

3. 通信方式の概要

開発元の異なる多種多様なIPコアの再利用にはインタフェースの標準化が不可欠である。そこで，オブジェクト指向技術で用いられているメッセージとパラメータから成るメッセージ通信とすることにより，IPコアの標準化が容易になる方式の研究を行ってきた。これにより，使用者は個々のIPコアの処理手順を知る必要はなく，メッセージを送るだけという統一した使用法で多種多様なIPコアを使うことができる。

IPコアとバス間に提案する通信制御機構(Access Control Unit : ACU) を各IPコアごとに配置し，開発元の異なる各IPコア間のインタフェースをとることでIPコアの再利用が容易になり，課題となっている各種IPコアの標準化の問題が解決できる。更に，チップ上でのネットワークを形成するにあたり，従来のバス形構成ではバス調停機構の問題が伴うが，コンピュータネットワークで用いられているトークン方式をACUの連携に用いることでバスの使用権を制御する。これにより従来のようなバス調停機構を用意する必要はなくなる。

ACUの特徴として，どのIPコアに対してもすべて全く同じアーキテクチャであり，接続するIPコアに合わせた設定をする必要は無く単純にIPコアと接続するだけでIPコア間の通信を行うことができる。

3.1 IPコア間の通信フォーマット

データ通信においては，IPコアの指定する相手のアドレスである論理アドレスを集積時に決定した物理アドレスに変換する必要がある。つまり，IPコアとACU

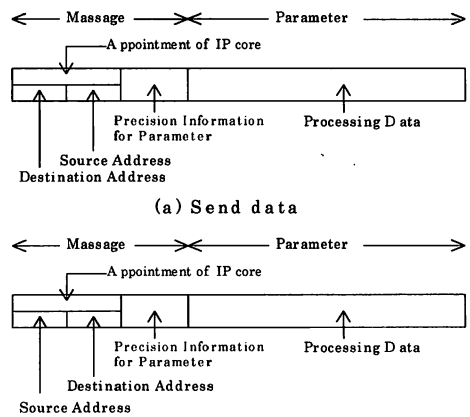


図1　ACU間の通信フォーマット

Fig.1 Send/receive data format between ACUs.

間ではIPコアの論理アドレスとACUの物理アドレスの変換が必要となる。ACU間の通信フォーマットを図1に示す。送信データのIPコア指定にはIPコアからの論理送信先アドレスをそのACUの物理アドレスに送信先アドレスとして付加し，続けて，送信するACUのアドレスを送信元アドレスとして付加して送信する（図1(a)）。指定したIPコアで処理された結果はIPコア指定の送信元と送信先アドレスを逆にして，バスに送出される（図1(b)）。

3.2 通信機構の概要

ACUの概要を図2に示し，以下に各機構の概要を述べる。

トークン制御機構はIPコアの通信要求の有無によってトークンを保持するか，パスするかを管理,および初期トークンを発生する機構である。集積時に任意に指定したひとつのACUで一定時間(時間は任意に指定できる)経過したら初期トークンを出力する。IPコアからの通信要求があり，トークン通知線からトークンが入力されたとき，IPコアへの通信許可を出力し，トークンを保持する。保持したトークンはデータ通信が終了したら次のACUへトークンをパスする。IPコアからの通信要求がなければ次のACUへトークンをパスする。トークンを確実にパスするため，トークン通知線とトークン終了検知線はハンドシェイク方式を採用している。これによりトークン通知線がアクティブになったら直前のACUのトークン終了検知線をアクティブにし，トークン通知を終了する。このトークンに相当するアクティブ信号をループ状にパスしていくことでバスの使用権を決定する。

また，なんらかのエラーでトークンが消滅してしまった場合，任意に指定した機構が一定時間経過することで新たなトークンを出力する(初期トークンの出力と同様な状態)。

アドレス変換機構はIPコアからデータを送信する場合，送信先のIPコアの論理アドレスをACUの物理アドレスに変換し，送信元のACUアドレスを付加して，オン・チップ・バスにデータを送出する。送信後，指定したIPコアからそのIPコアのACUに返送された処理結果は，アドレス判別機構で一時保存していた送信元アドレスを送信先アドレスとし，元々の送信先アドレスを送信元アドレスとして，オン・チップ・バスにデータを送出し，送信元のACUに返送する。

アドレス判別機構はオン・チップ・バスから送られてくるデータが自宛であるかを判別する。自宛でなければ続けて送られてくるアドレス以降のデータを無視する。自宛であれば，続けて送られてくるパラメータを取り込み，IPコアへ通信要求を出力する。IPコアから通信許可を得たら，送信元アドレスを取り除いてIPコアへデータを送出する。このとき取り除いた送信元アドレスは，IPコアで処理されたデータを送信元のIPコアへ返送するために一時保存される。

エラー判別機構はオン・チップ・バスへデータを出力すると同時に取り込み，オン・チップ・バスへ出力する前のデータと比較する。出力後のデータが出力前のデータと違っていたらオン・チップ・バス上でデータが衝突していると判断する。

これは本来1つであるべきトークンが誤動作で2つ以上存在してしまった結果，生じたことであるので，エラー検知線をアクティブにしてすべてのACUにエラー信号を送出し（トークンを保持しているACUはIPコアに対して精度情報を"0"として再送要求を行なう），ACUを初期化する（トークンを非アクティブに

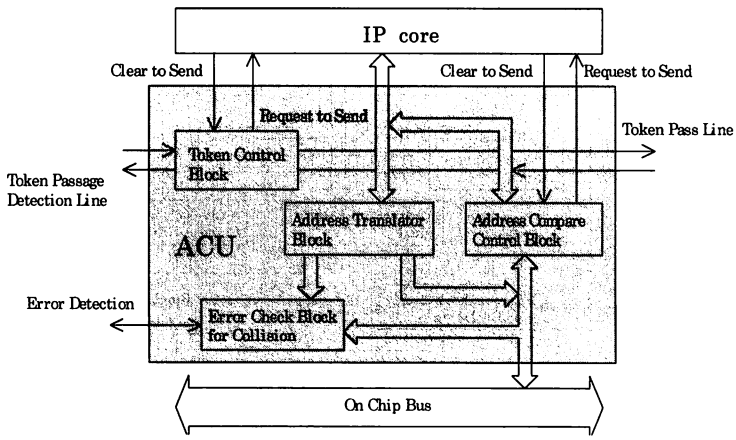


図2　ACUの概要

Fig.2　Outline of the ACU module.

し，トークンが全くない初期状態にする)。

4. 通信情報の暗号化

開発元の異なる多種多様な IP コアをひとつのチップに集積化する SoC において，SoC 内の通信データが盗視され，情報の漏洩やチップ内を解析されて IP コアが盗用されることが懸念されている。また，流通する多種多様な IP コアの使用に際して，IP コアが盗用される危険性を解決することは各開発元の信頼性向上のために不可欠である。

以上のような背景から SoC 内の各 IP コア間の通信データを隠蔽することを提案する。

その手法として， IP コア間の通信制御を行う ACU のオン・チップ・バス接続部分に暗号機構を挿入し，データバスの暗号化を行う。さらに，図 5 に示すようにすべての ACU と DES サーバの間に 1 本の信号線(データ送出信号)を追加した。これにより提案する同期回路部分のバスに送出されるデータをすべて隠蔽し，IP コアの盗用を防止することができる。

4.1 暗号システムの実装

DES を内蔵した ACU の概要を図 3 に，DES サーバの概要を図 4 に，DES サーバを配置した接続方式を図 5 に示し，以下に各機構の概要を述べる。

暗号機構は高速で秘密鍵暗号の標準となっている DES 暗号を採用する。IP コアから ACU にデータが入力され，オン・チップ・バスへ出力する際にそのデータを暗号化し出力する。また，オン・チップ・バスから入力されたデータを復号し，IP コアへ出力する。

DES サーバは各 ACU で使用される暗号用の鍵を管理する。暗号化された通信データが DES サーバへ入力後，復号され，送信先のアドレスを確認し，送信先の ACU 用の鍵で暗号化し，オン・チップ・バスへ送出する。

鍵判別機構はすべての鍵を保持しており，ACU から入力された通信データを DES で復号する際には復号鍵を出力し，その復号したデータを取り込み，そのデータ内の送信先アドレスを確認し，送信先用の鍵を DES へ出力する。

鍵交換機構はそれぞれの ACU 用の鍵を指定した回数以上使用後，トークン取得時にランダムに発生した新しい鍵を各 ACU へ送出する。また，DES サーバ用の鍵を変更する場合はすべての ACU が DES サーバの鍵で暗号化された鍵データまたは再送要求フォーマットを復号できるようにデータ送出線を非アクティブ状態でデータの先頭に 1byte の 0 を付加する。通常，バスにデータが送出されているときはデータ送出線がアクティブ状態となっているので通常の通信でデータの先頭が 0 となっていても DES サーバの鍵を全 ACU に送出するブロードキャストと誤判断することは無い。

4.2 通信手順

シミュレーション例を図 6 に示し，提案する通信機構の通信例として，図 5 における IP コア 2 から IP コア N へ通信を行う場合の処理過程を説明する。また，説明を容易にするために各 ACU に番号が割り振られているが，ACU はすべて全く同じモジュールである。

IP コア 2 から IP コア N へのデータは，IP コア 2 が ACU2 に通信要求信号を出力している状態で，ACU2 がトークンを取得することで ACU2 は IP コア 2 に通信許可信号を出力する。許可を得た IP コア 2 は接続されている ACU2 へデータを送出する。ACU2 はデータの送信先アドレス(論理アドレス:IP コア N のアドレス)

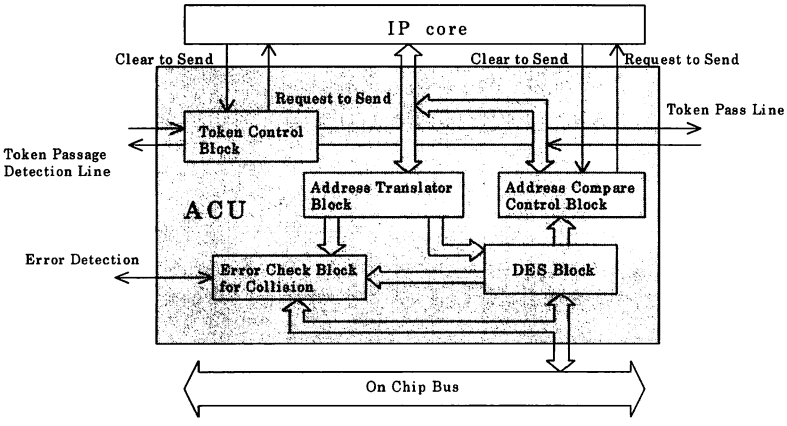


図 3　DES 機構を内蔵した ACU の概要
Fig.3　Outline of the ACU with DES function.

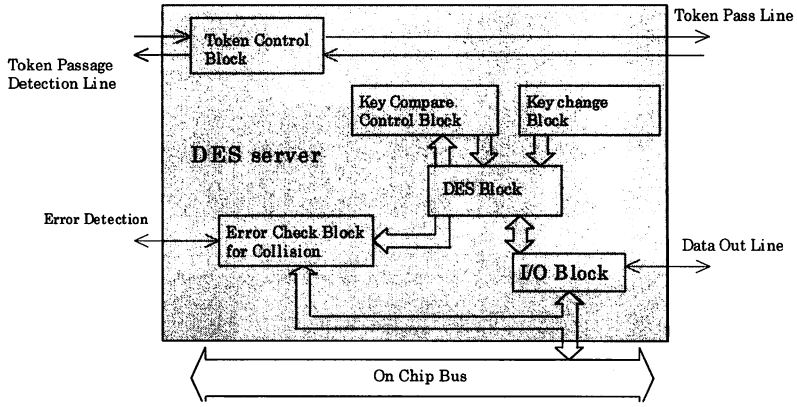


図 4　DES サーバの概要

Fig.4　Outline of the DES server module.

をオン・チップ・バス側アドレス(物理アドレス:ACU N のアドレス)に変換し，続けて ACU2 の送信元アドレスを付加したデータを内部で一時保存する。ACU2 はデータを DES 機構で DES サーバの鍵で暗号化し，オン・チップ・バス上に送出する(図 6(a))。送出している間データ送出線はアクティブとなる(bus_sw=0)。

復号できるのは DES サーバだけで，DES サーバは復号後データ内の送信先アドレスを確認し，送信先の持つ鍵を用いて再度暗号化を行いオン・チップ・バス上に送出する(データ送出線アクティブ(bus_sw=0))。すべての ACU が復号を行い，アドレスが一致(この場合 ACUN)したものだけが接続されている IP コアへ通信要求を出力する。IP コア N から通信許可が入力されたら，ACUN は送信元アドレス(IP コア間でのみ使われるデータ: この場合 IP コア 2)を取り除き，保存して IP コア N へデータを送出する(図 6(b))。IP コア N で処理されたデータは，接続されている ACUN へ返送され，一時保存していた送信元アドレス(IP コア 2 のアドレス)を処理後のデータの送信先アドレスとし，その送信先アドレスをオン・チップ・バス側のアドレス(物理アドレス:ACU2 のアドレス)に変換し，DES サーバの鍵で暗号化後オン・チップ・バス上に送出する(データ送出線アクティブ(bus_sw=0))。同様に DES サーバは復号後データを送信先の ACU2 の鍵で再暗号化し，すべての ACU が復号，アドレス判別を行う。アドレスが一致した ACU2 だけが IP コア 2 に通信要求を出力し，IP コア 2 から通信許可が入力されたら ACU2 はデータを IP コア 2 へ送出し，IP コア N で処理された結果が返送される。通信終了後，トークンはトークン通知線によって次の ACU である ACU3 へパスされる。これによって次は IP コア 3 がバスの使用権を得る。

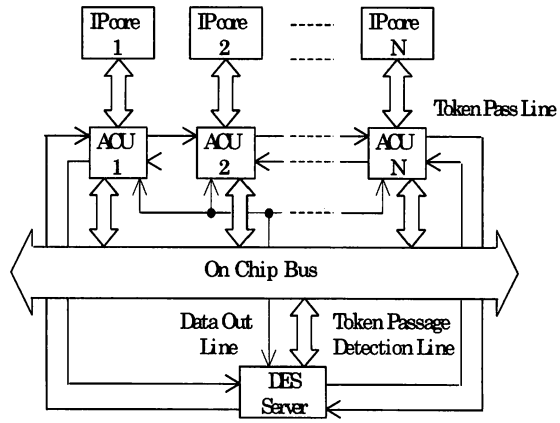


図 5　IP コアの接続方式

Fig.5 Connection outline of the IP cores

今回設計した各回路のゲート数及びターゲットデバイスを Xilinx 社の FPGAVertx-4 としたときの最大周波数を表 1 に示す。

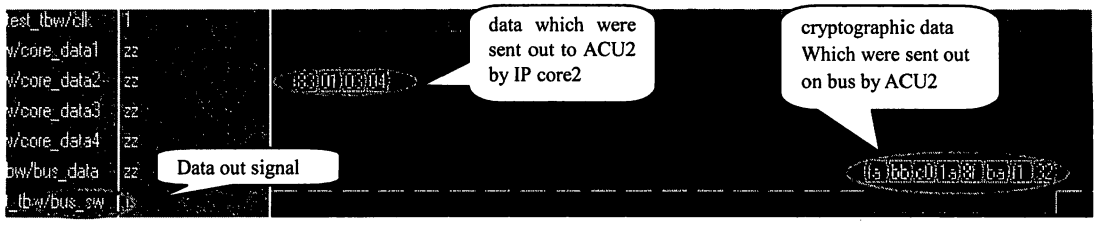
ACU と DES サーバにはそれぞれ DES 機構が内蔵されているが，ゲート数や処理速度の低下は問題となるほどではないと考える。

表 1　各回路の特性

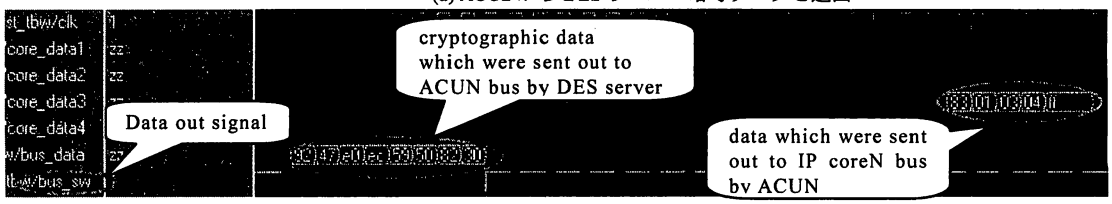
Table1. Characteristic of each circuit block

回路	ゲート数	最大周波数 (MHz)	入出力ピン数
ACU	18,314	100.403	45
DES サーバ	19,447	91.057	43
DES 機構	7,550	134.570	197

4.3 FPGA での試作



(a) ACU2 から DES サーバへ暗号データを送出



(b)DES サーバから IP コア N へ復号データの受信

図 6 暗号化/復号のシミュレーション例(IP コア 2 から IP コア N)

Fig.6 Simulation example for encryption/decryption (from IP core2 to IP coreN)

5. まとめ

IP コアのオブジェクト指向ハードウェア設計法によるインタフェースの標準化の問題を解決する通信機構（ACU）を用い，通信データの暗号化によって通信データを隠蔽し，かつ通信データ盗視による各種 IP コアの盗用を防止する一手法を提案し，それを実現するためのインタフェース機構の設計を行った。また，IP コアを 1 オブジェクトとして捉えることによってソフトウェアのように柔軟性のあるモジュールとして考えることができるため，新たに IP コアを付加しようとした場合でも容易に対応できる。オブジェクト指向ハードウェア設計法により使用者は内部仕様を知る必要がなく，多くの IP コアを容易に集積化および使用することが可能となる。

これからのシステム LSI や SoC においては，多くの IP コア間の通信方式が大きな課題となっており，様々な研究報告が見られる。中でも全体的に非同期式/局所的に同期式（GALS）が注目されている。本方式は局所的な IP コア間の暗号化通信方式としての提案である。

文献

(1) Luca Benini and Giovanni De Micheli : "Networks on Chips : A New SoC Paradaim", IEEE, Computer, pp.70-78, Jan 2002.

(2) P.P.Pande, C.Grecu, M.Jones, A.Ivanov and R.Saleh : "Performance Evaluation and Design Trade-offs for Network-on Chip Interconnect Architectures", IEEE Trans. on Computers, pp.1025-1040, Aug 2005.

(3) 唐木信雄：「非同期回路設計のすすめ」, Design Wave, 7, pp.64-69, Jul 2005.

(4) Rechard Goering:「次世代システム LSI の性能限界オン・チップ・バスが鍵を握る」, EE TIMES Japan, No.3, pp.32-33, Sep 2005

(5) Matthew W. Heath, Wayne P. Burleson, Ian G. Harris: "Synchro-Tokens: A Deterministic GALS Methodology for Chip-Level Debug and Test", IEEE Trans. on Computers, Vol. 54,No.12,pp.1532-1546, Dec 2005

(6) 安生健一郎・鯉渕道紘・山田裕・上楽明也・天野英晴：「ネットワークオンチップにおけるローカルラベリング方式の評価」, 信学論, D-I, Vol.J88-D-I, No.6, pp.1076-1090 (2005)

(7) 古屋憲吾・中村次男・冬爪成人・笠原宏：「オブジェクト指向技術を導入した IP コアの設計とその連携方式」, 電気関係学会関西支部連大 G10-15(2003)

(8) 早川雅文・中村次男・佐藤正幸・畠中浩行・冬爪成人・笠原宏・田中照夫：「SoC 内 IP コア間の通信方式」, 平成 17 年電気学会電子・情報・システム部門大, GS2-2, pp.764-750(2005)