

**次世代光通信ネットワーク用量子暗号化**

**光 WDM 送受信機に関する研究**

**Studies on Quantum Encryption Optical WDM Transceiver for the Next  
Generation Optical Communication Network**

**2008 年 3 月**

**原 澤 克 嘉**

## 目次

第1章	緒言	1
1.1	本研究の背景	1
1.2	本研究の目的	2
1.3	本論文の構成	2
第2章	将来光通信システム（将来光通信システムの概要と課題）	4
第3章	自律制御型 WDM 光伝送装置の開発	6
3.1	緒言	6
3.2	インテリジェントアーキテクチャの基本コンセプト	9
3.2.1	基本コンセプト	9
3.2.2	新技術と従来技術の相違点	10
3.2.3	新アーキテクチャの導入効果	11
3.3	新アーキテクチャの光通信制御アルゴリズム	12
3.3.1	光送受信機のハードウェア構成	14
3.3.2	波長および光出力電力自動制御アルゴリズム	20
3.3.3	波長検出	21
3.3.4	エタロンフィルタの温度依存性の補正方法	22
3.3.5	LD の波長制御精度	22
3.3.6	LD の温度制御精度	23
3.3.7	光伝送特性の最適化手法	23
3.4	新アーキテクチャの機能検証実験結果と考察	24
3.4.1	波長制御	25
3.4.2	光出力電力制御	30
3.4.3	波長および光出力電力制御総合検証実験結果	31
3.4.4	光出力波形制御	32
3.5	自律制御アーキテクチャのシミュレーションによる検討	33
3.5.1	シミュレータ	33
3.5.2	光出力制御ループのモデル化	34

3. 5. 3	シミュレーション結果および考察	35
3. 5. 4	ループ応答の高速化	37
3. 5. 5	光波長制御ループのシミュレーション解析結果	40
3. 6	システム LSI の方式および要素回路の開発	40
3. 6. 1	システム LSI の構成と開発課題	40
3. 6. 2	EA-Driver 回路	43
3. 6. 3	分周器	47
3. 6. 4	ハーフレート方式	50
3. 6. 5	小型、低消費電力 MUX 技術	53
3. 7	LSI 化のための要素回路 TEG の試作、評価	55
3. 7. 1	チップダイシングと評価基板実装	56
3. 7. 2	チップダイシング	57
3. 7. 3	ダイスボンディング	59
3. 7. 4	ワイヤボンディング	59
3. 7. 5	要素回路 TEG の評価結果	61
3. 8	システム LSI の試作・評価	69
3. 8. 1	MPU の開発	70
3. 8. 2	試作・評価結果	74
3. 9	まとめ	78
第4章	光通信量子暗号伝送装置の開発	79
4. 1	緒言	79
4. 2	光通信量子暗号 (Y-00) 方式の暗号化原理	81
4. 2. 1	暗号化原理	82
4. 2. 2	基底の概念	84
4. 3	Y-00 暗号化光送受信機の構成	88
4. 3. 1	光受信部	88
4. 3. 2	光受信部	89
4. 3. 3	多値変調／復調回路	90
4. 3. 4	多値変調部の詳細設計	93

4. 3. 5	ランダムシフター	95
4. 4	Y-00 光送信機、受信機の試作結果	104
4. 4. 1	基本特性	104
4. 4. 2	安全性の評価	105
4. 5	Y-00 トランシーバの開発	107
4. 5. 1	Y-00 暗号化変調回路	107
4. 5. 2	多値変調回路	108
4. 5. 3	受信機 (復調回路)	110
4. 5. 4	トランシーバの試作結果	110
4. 6	伝送実験	113
4. 7	10Gbit/s Y-00 伝送装置の開発	117
4. 7. 1	高速化の検討	117
4. 7. 2	回路設計	118
4. 7. 3	DAC IC の試作結果	125
4. 8	まとめ	132
第5章	結 論	133
	謝 辞	134
	参考文献	135

## 第1章 緒論

### 1.1 本研究の背景

1990年代半ばからインターネットは急速に普及し始め、通信は音声中心からPCデータを中心とする情報通信が主流となった。このインターネットは更に発展し、画像伝送を中心とする情報の大容量化が進み、これら通信を支えているネットワークも世界規模で急激に大きな変化を遂げてきた。音声やFAXデータ中心の時代のネットワークは、端末や加入者レベルで扱うデータ量は限られていたためネットワークは階層型で構成されており、上位階層ほど伝送容量は大きくなると、大都市間などの主軸のバックボーンでのみでGbit/s帯の大容量光通信伝送が行われていた。しかし、前述のように、動画画像や大容量のPCデータなどを個人レベルで扱うようになり、アクセス系のブロードバンド化へのニーズが急速に高まってきた。それらを支えるネットワークは、階層型からスター型へ移行され、更に複雑なネットワーク構成へと進んでいる。またネットワークのトラフィックは日々増大しており、特にバックボーンネットワークの伝送容量不足が危惧されだしている。現在このネットワーク回線容量を10～100倍に引き上げるため、その大容量化には、10Gbit/sの伝送を基準とした光の波長分割多重（WDM : Wavelength Division Multiplexing）方式が一般的に用いられており、総伝送容量がTbit/s級の大容量ネットワークの構築が積極的に進められている。一方、光伝送システムにおけるコスト低減の要求は非常に厳しい。特にWDM用送受信装置には光源の波長や光強度の安定化が厳しく要求されるので、光素子特性の製造バラツキ、温度変動、各光素子間の温度特性バラツキなどを吸収できる補正回路の適用、固体ごとの調整が必要不可欠となるため、光送受信装置のコスト低減は困難であり、システム普及の妨げになっている。これらの問題を解決し、光送受信装置の大幅な低コスト化を可能とする技術開発が急務となっている。

また、情報ネットワークを利用したアプリケーションも多岐にわたり飛躍的に拡大・発展し、インターネットを中心に、ネットバンキング、ネット決済、ネット取引等のビジネスが急速に普及し始めている。更に金融情報や個人情報などを初めとする機密情報伝達にも積極的に利用されるようになってきた。このため、ネットワークの安全性が強く意識されるようになり、次世代に向けたネットワークでは、従来の上位レイヤで行われていた数理的

な安全性だけでなく、伝送系の下位レイヤでも物理的に安全性を保証できるネットワーク構想が開始されだしている。現在のネットワークにおける情報の安全性保護には様々な数理暗号（数学的に計算の複雑性を利用した計算量的安全性を求めた暗号）が用いられてきている。しかし、これら数理暗号は将来コンピュータの処理能力の向上や暗号解読アルゴリズムの発見により安全性の低下は避けられない。これらを解決するため量子情報通信分野でも特に実用化に期待の持てる量子暗号の適用が考察されてきている。

## 1. 2 本研究の目的

前項で述べたように、ネットワークの大容量化の要求を満足し、更に幅広く普及させて行くためには、WDM光伝送用光送受信機の高密度多重化と低コスト化は必須である。また、同時にネットワークを流れる情報の安全性確保のために、従来一般的に利用されている上位レイヤでの数理暗号によるデータ保護だけでなく、下位（物理）レイヤで直接、物理的な伝送系の保護の要求が大きくなってきている。本研究の目的は、これら次世代に向けた光通信システムの2つの要求を満足させるため、①従来のWDM用光送受信機の高密度大容量化とコスト低減を目的に、新たな制御手法を取り入れた自己学習、自律制御並びに自己診断できる機能を具備するインテリジェントアーキテクチャを提案した。また、この手法の実現性を確認するために、回路のLSI化を行い、実証実験を行った。更に②ネットワーク情報の安全性確保のため、回線保護を目的とした、光通信量子暗号（Y-00）の理論を応用した暗号化光送受信機を開発し、その実用化への見通しを検討することにある。

## 1. 3 本論文の構成

本論文の構成について述べる。本論文は将来の光通信ネットワークに要求される課題を解決する光送受信機を提案し、装置の開発および検証実験での試作結果を通して実現の見通しを検討し、その技術をまとめたものである。

各章の構成は以下の通りである。

- ・第2章 将来光通信システムの概要と課題

現在、盛んに考案され実現されつつある次世代ネットワークと、更にその先で展開される将来の新世代ネットワークが考案されている。これら将来の光通信ネットワーク構想を

考察し、その概要と技術的な課題について述べる。特に本論文の中心である、大容量光伝送の方向と、情報ネットワークの安全性を中心にまとめる。

- ・第3章 自立制御型WDM光伝送装置の開発

この章では将来の大容量光伝送の問題点を解決するために、高密度光WDM伝送に適した新たな光送受信機の自律制御型アーキテクチャを提案し、更に、このアーキテクチャを利用した光送受信機を試作し、検証実験結果を基に、その実現化への検討結果について述べる。

- ・第4章 光通信量子暗号伝送装置の開発

本章では、光通信ネットワークにおいて、もう一つの課題である情報セキュリティの確保に対して、光の量子効果を応用した新たな光通信量子暗号理論を具現化した暗号化光伝送装置の技術開発について述べ、また試作した装置を用いた商用回線を利用した伝送実験結果から早期実用性への検討結果について述べる。

- ・第5章 結論

各章での研究成果をまとめ、将来の光通信システムを考慮し、新たに考案した光送受信機有効性および早期実現性について総括する。

## 第2章 将来光通信システム（将来光通信システムの概要と課題）

総務省は、IP（Internet Protocol）をベースとした次世代ネットワーク（NGN：Next Generation Network）構想の実用化試験を進める一方、従来のプロトコルやシステムにとらわれない全く新しいネットワークアーキテクチャを新世代ネットワークとして将来（2015年）の実現に向け、構想を始めている。このネットワークは、インターネットでの限界を超えた新たな発想に基づいたアーキテクチャの確立を考えている。この構想の中で新世代ネットワークに対する社会的な要求として上げられている幾つかの項目の中で、以下のような強い要望もある。

### （a）ネットワークの大容量化

ペタビット級のバックボーン、100GbE（10Gbit/s イーサネット）、10Gbit/s FTTH（Fiber To The Home）など。

### （b）ネットワークのセキュリティ強化

安全、安心（プライバシー、金融等）。

（a）においては、インターネット利用の拡大と、ネットワークで扱う情報（動画コンテンツ等）の大容量化でIX（Internet Exchange point）のトラフィックの増大に伴い、その容量は、現在でも100Gbit/s以上なければ収容できないほどになっており、更に10年後には100Tbit/sオーダーに達することが予測されている。また、FTTHにおけるアクセス網は、10Gbit/sの要求が強くなり、現在Tbit/s級のハイエンドルータの交換容量は、2015年にペタビット（Pbit/s）級のルーターが必要とされ、このときのデータリンクの速度は10Tbit/sになると推測される[1]。

これらの推測に基づき、様々な方式の大容量光伝送装置の開発が盛んに行われている。伝送速度を上げる手法としては、①光送受信機の高速度化、②WDMの多重数の増加、の2つの方向がある。現在の光強度変調を基本とした伝送装置では、40Gbit/s以上の高速伝送においては光ファイバケーブルの分散特性等の影響により伝送距離を伸ばすことが困難になっている。このため40Gbit/s以上の高速・長距離伝送には、位相変調を利用した方式の提案が検討されてきている[2]。しかし、FTTHにおけるアクセス系などを中心に要求される光送受信機では装置の低価格化を考え、更に既存のインフラや装置との親和性を考慮すると10Gbit/sをベースにしたWDMの多重数を増やしていくことが必須である。現在のシステムの波長多重数は100波長程度であるが、将来的には25GHz間隔の1000波長の多



重が必要と考えられている[3]。また、現在、開発が進められている全光パスネットワークでは、個々の光信号の波長や波長数を自由に制御し、スイッチングやフィルタリングすることが必要であり、更なる波長数を増大する新技術（スーパーコンティニウム技術）を用いた 10000 波以上の波長の光を発生させる実験も成功している[4]。このように多重する光信号の波長間隔は可能な限り狭くする必要があり、高精度な制御を可能とする光送受信機の開発が必須である。

(b) のネットワークの安全性においては、物理的な手段を考えて行く必要がある。現在使われている数理論号（3DES : Triple DES、RSA 暗号など）は、暗号の 2010 年問題（米国政府の暗号基準を考え、現在一般的に使われている数理論号を 2010 年までに、より安全なアルゴリズムの暗号へ移行する計画）等の例にあるように、将来コンピュータの処理能力の向上や、解読アルゴリズムの発見により安全性を失う恐れがあり、常に改良、改版して行く必要がある。このような安全性への不安を解消するためには、物理現象を利用して解読することが困難であり、安全性を保証できる量子暗号に期待がもたれている。量子暗号は、光の量子性（量子の不確定性原理）を利用し、情報を盗聴できないようにする暗号である。

### 第3章 自律制御型 WDM 光伝送装置の開発

#### 3.1 緒言

ブロードバンドインターネットサービス等の急速な普及を支えるために Tbit/s 級の波長分割多重 (WDM) 伝送を利用した大容量ネットワークの構築が積極的に行われてきた。この大容量化を実現しているのが光波長多重 (WDM) システムである。一般的な WDM システムの概念を図 3.1 に示す。

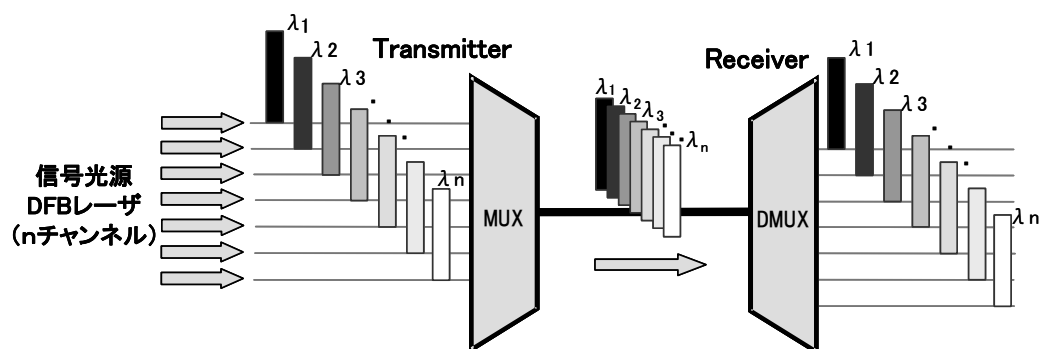


図 3.1 一般的な WDM システム

多重する光の波長間隔は、ITU-T (International Telecommunication Union Telecommunication Standardization Sector) の国際標準規格で定められており、図 3.2 のように C-WDM (Coarse-WDM) では 20nm の波長チャンネル間隔であり、D-WDM (Dense-WDM) では最高 100GHz の波長チャンネル間隔である。これらの波長間隔の定義は、C-WDM、D-WDM で違い、C-WDM での波長間隔は、波長を多重・分離するフィルタの中心波長で規定され、また D-WDM では、193.1THz を中心に 12.5GHz、25.0GHz、50GHz、100GHz 間隔のいずれかで規定されている[12]。

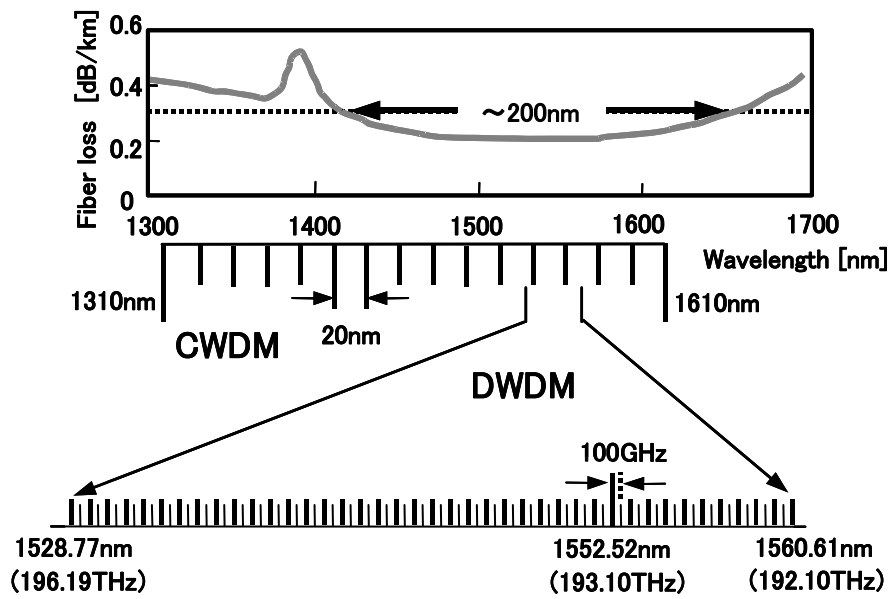


図 3.2 波長グリッド

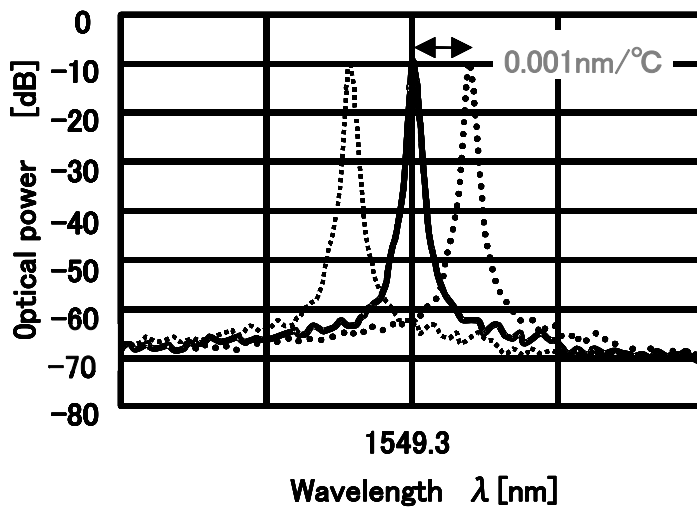


図 3.3 LD 発光波長の温度依存性

これらのシステムを実現する光 WDM 用送受信機の送信部は、隣接しあう波長での LD (Laser Diode) 光スペクトルが重ねあわないように設定する必要がある。図 3.3 に一般

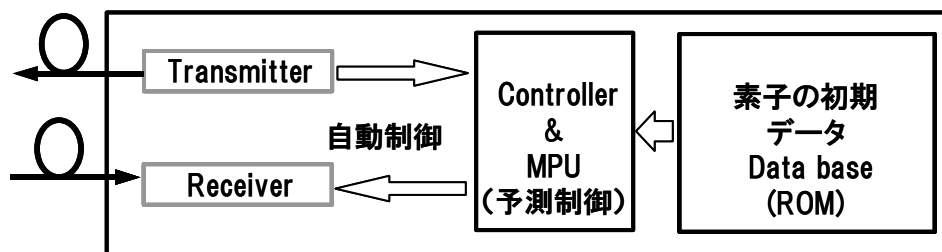
的な WDM 用光送信器で用いる DFB-LD (Distributed Feedback Laser Diode) の波長特性を示す。WDM 伝送における光送信器は波長の精度と安定性を保つことが重要である。しかし図からもわかるように LD の波長は動作中の環境温度に大きく依存 (0.001nm/°C 程度) する。逆に温度を決定すれば波長は常に一定であり、LD の動作温度をコントロールすることにより波長を安定させることが可能である。しかし、安定な光伝送を行うためには、光素子 (特に LD) の特性の製造バラツキや温度変動等の環境変化による特性変動を吸収する補正回路の適用や、光送受信機の個体毎の調整作業が不可欠である。また従来の光送受信機では、一般に、ROM に書き込んだ光素子の特性データの初期値のみで条件設定することが行われてきたが、長期間に亘って安定な性能保証を得るため、光素子個々について、特性の製造バラツキや温度変動などの詳細なデータ取得が必要であった[5][6][7][8]。それ故、光素子の初期特性データの取得や専門技術者による高精度な調整作業に数時間を要し、光送受信機のコストの高騰を招く大きな要因になってきた。更に、従来の光送受信機では稼動中に随時 ROM データを書き換えられないため、経時変化を監視して自己診断・自律調整する機能が無く長期信頼性の点で課題があった。そこで、本研究では常温におけ基本的な光素子特性を測定し、そのデータを初期値として設定するのみで、その後は光素子の詳細データを自己取得して RAM に書き込み、現状データの保存と稼動中の制御データの随時書き換えが可能な自己監視・自律調整機能を具備するインテリジェントアーキテクチャの開発を進めてきた[9]。このアーキテクチャの特長は、光送受信機の運用中においても常に装置内の特性変化を抽出・蓄積 (自己学習機能) し、そのデータを基に特性劣化の補償を行うことで、光送受信機を常に最適動作状態に自律的に制御 (自律制御機能) できることにある。これにより調整作業が不要となり、コストの大幅な低減が可能となると共に装置自体で経時状態を自己診断できる機能を持たせることができる。

本章では、3. 2項で提案するインテリジェントアーキテクチャの基本コンセプトについて述べる。次に、3. 3項では、基本コンセプトを具現化する手法 (制御アルゴリズム) について詳述する。3. 4項では、提案アーキテクチャ実現のフィージビリティを確認するために行った検証実験の結果について述べる。3. 5項では、提案するアーキテクチャのシミュレーションによる検討結果を述べ、3. 6項ではシステム LSI の方式および要素回路の開発について述べ、更に3. 7項で要素回路の TEG 試作と評価結果、3. 8項でシステム LSI の試作を述べる。3. 9項では、本章の結果を要約する。

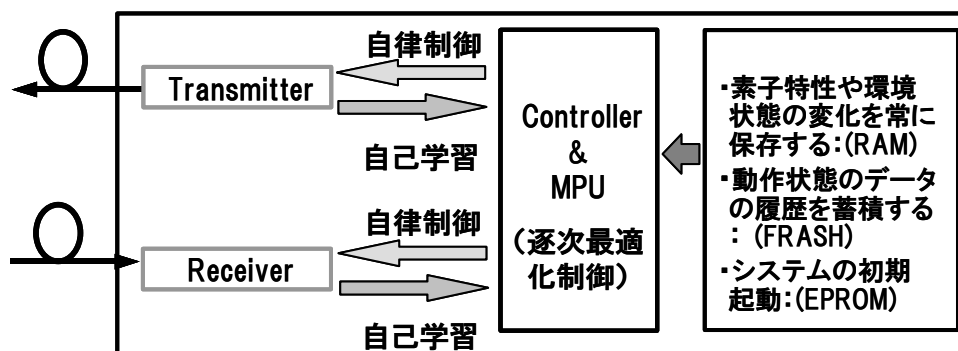
## 3. 2 インテリジェントアーキテクチャの基本コンセプト

### 3. 2. 1 基本コンセプト

図 3.4 にインテリジェントアーキテクチャの基本コンセプトを示す。図 3.4 (a) は従来の一般的な光送受信機の基本アーキテクチャを示したもので、最初に、光素子、特に、LD の製造バラツキや温度変動に関する諸特性を詳細に測定し、得られたデータを初期データとして ROM に書き込む。次に、ROM データに基づいて LD の状態を決められた条件に設定する。初期データの項目としては、光波長、光出力電力-駆動電流特性、閾電流、微分量子効率およびそれらの温度特性等が挙げられる。この従来アーキテクチャでは、初期データが ROM に書き込まれた以降は光送受信機の稼働中のデータ補正が困難であり、オープンループ系となるため、従来から用いられているアナログ系の帰還ループを併用して補償を行っている。[10][11]。従って、初期データと実動作との誤差の自動補正や光素子の経年変化の状態把握、性能劣化の抑圧等が難しいといった欠点があった。図 3.4 (b) は光送受信機の新アーキテクチャの基本的な機能を示したもので、マイコン制御を利用したクローズドループ系の構成となっている。最初に、常温における LD の光波長、光出力電力-駆動電流特性、閾電流、微分量子効率等を自動的に検出し、初期データとして RAM に書き込む。これら初期データ以外は、光送受信機が自らシステム稼働中に環境条件（温度、電源電圧等）を把握すると共に、その時の波長や光出力電力等を逐次取得し、メモリにデータ蓄積する。次に、このクローズドループを介して、蓄積データを基に作成された特性マップとデータ履歴から最適制御条件を自律的に抽出して速やかに規格値に収束させる制御を行う（自律制御）。更に、経年変化の状態を常時判断し、その時間的变化量が予め設定した限界点を超えると、故障モードと判断してアラーム送出を行う（自己診断）。それ故、新アーキテクチャによれば、光送受信機は自らの状態を常に自律監視・制御すると同時に自己診断・学習する機能を具備したものとなる。



(a) 従来のアーキテクチャ (Open Loop Control)



(b) 新たに提案するアーキテクチャ (Closed Loop Control)

図 3.4 新アーキテクチャの基本コンセプト

### 3. 2. 2 新技術と従来技術の相違点

表 3.1 は、提案する新技術と従来技術との特徴の比較結果を示したものである。新技術では、光送受信機自身が RAM や FRASH、EPROM 等のメモリを介して自己管理およびデータの蓄積を行なう。また、常に最適状態で光送受信機を稼働させる自己学習能力を持つ自律監視制御アーキテクチャにより、LD 性能の大きな製造バラツキや温度特性のバラツキを吸収すると共に個別調整作業時間の短縮を行う。即ち、高精度な調整を短時間で行えるので、大幅なコスト低減をに期待が持てる。また、環境変化や経年劣化耐力が強く、自己学習機能により高精度、高信頼のシステムを実現できる。

表 3.1 新アーキテクチャと従来アーキテクチャの特長比較

項目	新アーキテクチャ	従来アーキテクチャ
監視、制御の構成	<ul style="list-style-type: none"> <li>・逐次データを書換え記憶</li> <li>・自己監視とクローズドループ制御</li> </ul>	<ul style="list-style-type: none"> <li>・登録されている初期データでのオープンループ制御が基本</li> </ul>
LDの製造上の特性ばらつきと環境変化による特性ばらつきの自律制御機能(記憶)	<ul style="list-style-type: none"> <li>・有り (RAM, FRASH, EPROM)</li> <li>・広い調整範囲</li> </ul>	<ul style="list-style-type: none"> <li>・無し(ROMのみ)</li> <li>・調整範囲が狭い</li> </ul>
LDの経年劣化に対する永続的補償機能	<ul style="list-style-type: none"> <li>・強い(校正機能つき)</li> </ul>	<ul style="list-style-type: none"> <li>・弱い(校正機能無し)</li> </ul>
測定および調整機能	<ul style="list-style-type: none"> <li>・LDの基本特性の自動測定</li> <li>・ROM、RAMへの書込</li> </ul>	<ul style="list-style-type: none"> <li>・LDの基本データ評価と温度特性</li> <li>・ROMへの書込み</li> <li>・個別調整が必要</li> </ul>
調整時間	約10分	約540分

### 3. 2. 3 新アーキテクチャの導入効果

図 3.5 に新アーキテクチャの詳細な内容とその導入効果を示す。図 3.5 (a) の従来アーキテクチャは実際の光送信機の一具体例を取上げたもので、LD 特性の初期データ取得および ROM への書き込み、設定の作業手順を経た後、ROM データに基づいて調整作業に入る。調整内容には、LD 特性、光出力電力、波形、伝送特性、警報監視機能等多くの調整項目がある。このため、1 台の光送受信機の調整に累計で数時間を要する。これに対し、図 3.5 (b) の新アーキテクチャでは、LD の基本データの取得簡素化による設定時間の短縮と時間を最も要する調整作業を MPU 制御で自動化し、無調整化することで、光送受信機 1 台当たりの調整時間を約 1/10 程度に低減することが可能となる。更に、新アーキテクチャを実装したインテリジェント LSI の開発により、従来の光送受信機のコストを 1/2、容積を 1/3 に小型化できる可能性を秘めている。

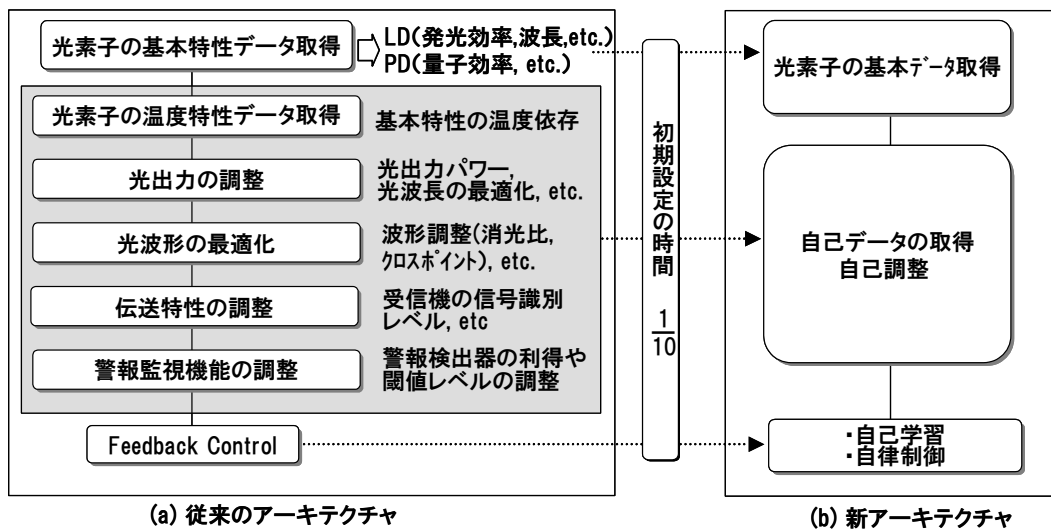


図 3.5 新アーキテクチャの導入効果

### 3. 3 新アーキテクチャの光通信制御アルゴリズム

光 WDM 用送信器では、光出力電力の安定化に加えて、波長の高精度化および安定化が鍵となる。しかし、LD の場合、波長は動作中の環境温度に大きく依存し、一般に、約  $50\text{pm}/^\circ\text{C}$  の割合で変動する。従って、LD の動作温度を制御して波長を安定化させることが必須となる。本研究では、光送受信機の製造過程におけるコスト低減を実現するために、光送受信機自身で高精度な最適化調整・制御を可能とする自己学習型のインテリジェントアーキテクチャを確立する。本章では、提案する新アーキテクチャを具現化するために試作、評価を行った光 WDM 伝送システムに対応する 10Gbit/s 光送受信ブレッドボード実験機の制御アルゴリズムについて述べる。また、そこで得た成果を用い、主信号系と制御系を集積したシステム LSI の開発に向け、その要素回路技術の有効性についての検証を行うため、試験用のシステム LSI を設計・試作を行った結果について述べる。

図 3.6 に提案する自律アーキテクチャの一部を示す。基本的な流れとしては、自己システム（伝送装置自体）の各種ユニークな特性を自己抽出し、評価システム（各種測定器）と連動したシステムを用いて、各特性の絶対値との相関を確認する。この相関データを



基に自己特性の検出データおよび検出システムの補正を行い、仕様に対する目標特性を満足できるように検出感度や調整感度の設定を行う。これらの基本データや初期の設定値はデータ化され、伝送装置内部のメモリにデータベースとして格納される。伝送装置は、初期動作時にこの基本データを基に動作の初期設定を行い、動作を開始するが、動作継続中は定期的に自己動作状態を検出することで常に状態の変化を確認し、その時点での最適動作状態になるよう各調整パラメータの調整を行う。このため光伝送装置は、光素子等の個別特性の経年劣化や動作環境条件の変化に対して精度の高い特性を維持することが可能となる。

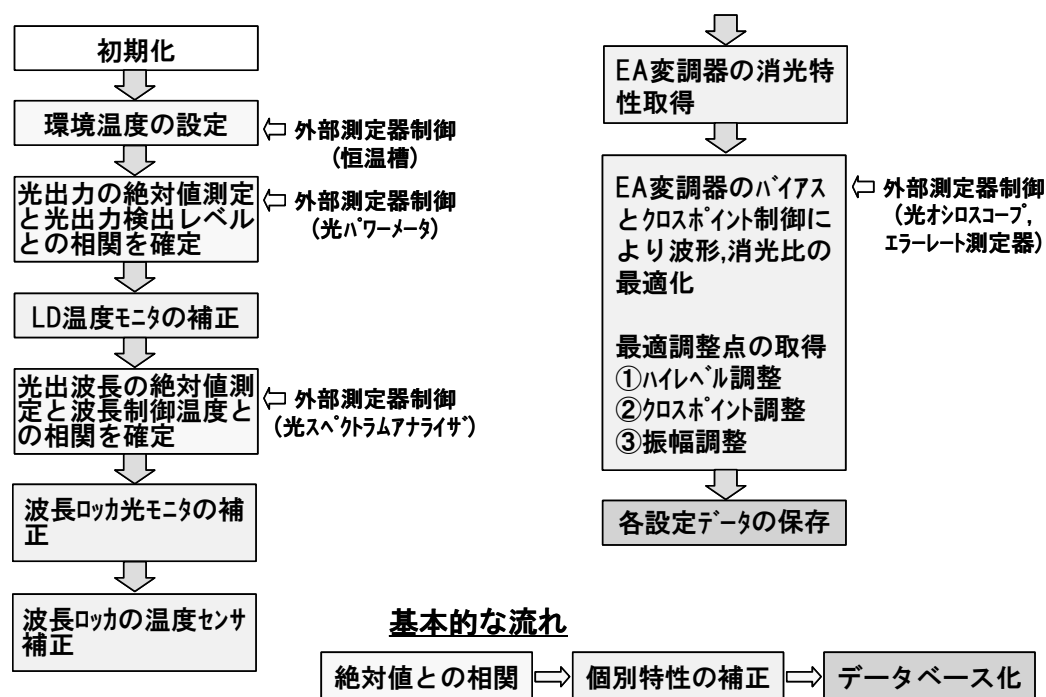


図 3.6 自律アーキテクチャの一例 (初期データの自動取得とデータベース化)

### 3. 3. 1 光送受信機のハードウェア構成

提案したアーキテクチャの検証実験において、光送受信機は世界標準を視野に入れ ITU-T 規格を基に目標仕様を決定した。表 3.2 に示す仕様を目標とした。

表 3.2 アーキテクチャ検証実験目標仕様

項目	目標仕様			単位	備考
	Min	Typ	Max		
中心波長	1535.0164	1535.04	1536.063	nm	ITU-T G692
波長安定度	-3		+3	GHz	
光出力パワー	0	+1	+3	dBm	
光出力波形	ITU-T G691 S-64 (b) 準拠				
温度	5	25	75	°C	
電源電圧		3.3/-5.2/5.0		V	

図 3.7 はブレッドボード実験機のブロック構成を示したもので、アナログ部（送受信部）とデジタル部（集中制御部）および周辺測定器にて構成している。送信部では、2.5Gbit/s 4 本の入力信号が MUX/DMUX（Multiplexer/Demultiplexer：信号多重/分離回路）にて 10Gbit/s に 4：1 多重され、Transmitter（光送信回路）に入力される。送信部では光出力制御、波長制御、消光比や光波形の最適化のための高精度な自動制御が行われ、EA-DFB-LD（EA 変調器+LD）から出力される強度変調光が光ファイバ伝送路に送出される。Receiver（受信回路）では、光ファイバ伝送路より入射された光信号が受光素子 PD（Photo Diode）および前置増幅器（Pre-amp.）で光－電流－電圧変換され、更に、AGC amp.（Automatic Gain Control Amplifier：利得可変増幅器）で等化増幅される。その後、CDR（Clock Data Recovery：クロック・データ再生回路）にてタイミング抽出と”1”、”0”の符号識別再生が行われ、10Gbit/s の受信信号は、MUX/DMUX 部

にて 4 本の 2.5Gbit/s 信号に分離し出力される。デジタル系の集中制御部は、MPU、Memory（メモリ）および Logic 部で構成されている。MPU からの制御信号で Control Interface (A/D, D/A を利用した制御インタフェース) を介して光出力、波長、環境温度、信号エラーおよび受信レベル等のアナログ回路の動作情報を取得し、この情報を基に演算した結果を用いて光出力、波長、波形や消光比などの調整のためアナログ回路がデジタル制御される。

a) アナログ部

図 3.7 の吹き出し付き矢印は、MPU がファームウェアにて処理し、自律制御を行う部分である。各部の主な動作は以下の通りである。

1) 送信部の詳細

(i) 図 3.8 は図 3.7 の光送信回路の詳細な回路構成を示したものである。APC (Automatic Power Control : 自動光出力電力制御) 回路は、CW (Continuous Wave : 連続発振) 光を発する LD の光出力レベル安定化のため、駆動電流の最適制御を行う。尚、LD 駆動電流は、LD 出力光の波長にも依存するため波長調整との関係が必要となる。

(ii) EA-Driver (外部光変調器駆動回路) は、初期データと動作状態のモニタ情報を利用・演算し、MPU からの光波形をモニタした制御情報を基に光出力波形のハイレベル、クロスポイント、信号振幅を調整し、光出力波形や消光比の最適化を行う。

(iii) Wavelength Fluctuation Detector (波長変動検出部) では、初期設定波長のずれが波長フィルタ機能を具備する波長ロッカーにて常に検出され、ATC (Automatic Temperature Control : 自動温度制御) 回路により出力波長の安定化が図られる。

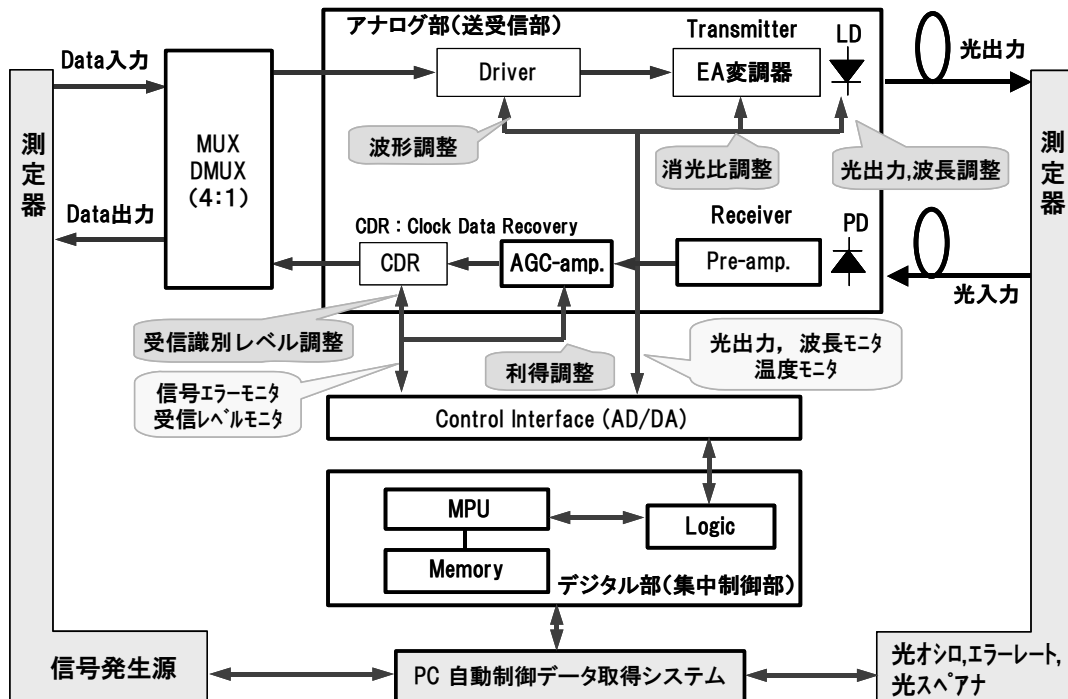


図 3.7 ブレッドボード実験機のブロック構成

## 2) 受信部

(i) 図 3.7 の Pre-amp (前置増幅器) は、光受信信号を増幅すると共に、光受信電流のモニタ結果から検出される異常現象に対応して ALM (アラーム) を発する機能を有する。

(ii) AGC 増幅器は、受信信号の信号レベルを検出し、常に出力振幅が一定になるようにし受信信号レベルの変動を吸収すると共に、信号レベルが極端に劣化したときに信号断検出とアラーム送出 (LOS-ALM) を行う機能を有する。

(iii) CDR は、受信信号の” 1”、或いは、” 0” レベルの最適識別を行うための信号検出閾値の最適調整 (Vth Cont) 機能およびクロック抽出機能を持ち、更に、常に受信感度が最適になるよう識別タイミングの位相調整機能を有する。

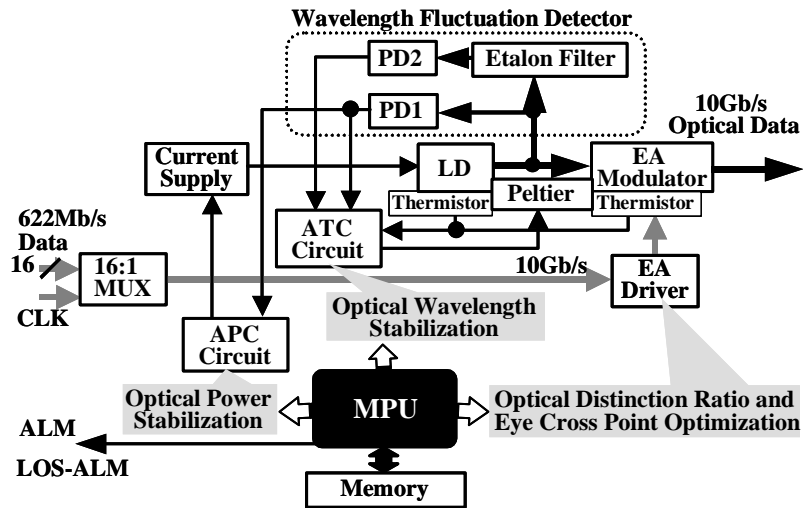


図 3.8 光送信機のハードウェア構成

b) デジタル部

図 3.9 にデジタル部の詳細を示す。デジタル部は、アナログ部からの各種検出データを制御インタフェース部で A/D (アナログ/デジタル) 変換されたデジタルデータを基に MPU を介して各種制御データを生成する。この制御データは、制御インタフェース部で D/A (アナログ/デジタル) 変換され、アナログ部の各機能を最適化する。また、取得した各データを元にメモリ上に新たなデータベースを構築する。ブレッドボード試作では、MPU、メモリ以外のデジタル回路は、FPGA (Field Programmable Gate Array) で構成した。

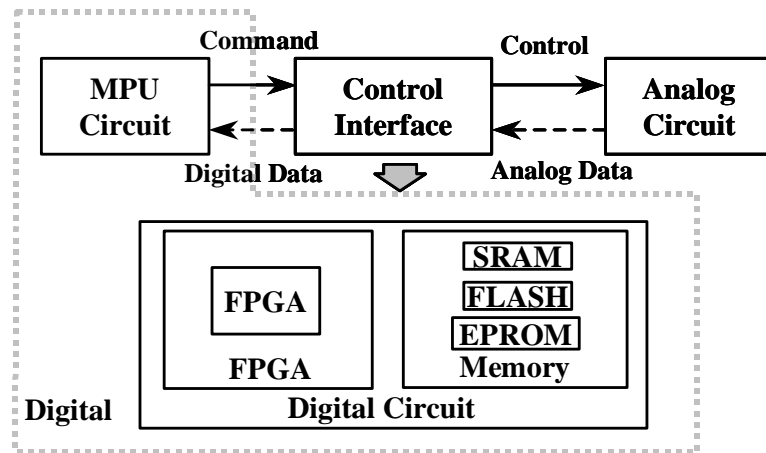


図 3.9 デジタル部の位置付け

### 1) FPGA 回路

FPGA 内部では、MPU から供給されるクロック信号をアナログ回路の制御に用いるための分周を行う。また MPU から各コマンドを読み込み、それに応じたアナログ回路との間で制御信号を送受する。更に MPU から各コマンドを読み込み、それに応じてメモリ回路との間で信号を送受する。

図 3.10 に FPGA の機能ブロック図を示す。FPGA は外部接続された MPU 部である SH マイコン（組込制御用マイクロコンピュータ）で各種のコントロールを行う。また、アナログ回路部とは ADC（Analog Digital Converter : アナログ/デジタル変換器）、DAC（Digital Analog Converter : デジタル/アナログ変換器）と DPM（Digital Potentiometer : デジタルポテンションメータ）を介して光送受信機の諸特性を観測し制御を行う。

FPGA の各内部機能を表 3.3 にまとめる。

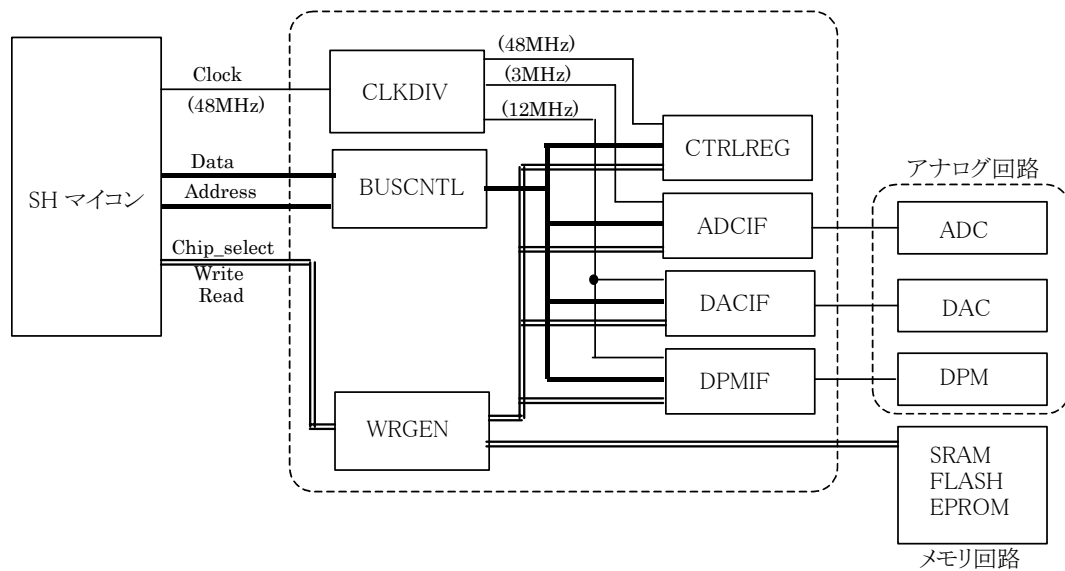


図 3.10 FPGA の機能ブロック図

表 3.3 F P G A機能の内容

ブロック名	機能名	機能の内容
CLKDIV	クロック分周器	クロックを $n$ 分周して各モジュールに対して必要なクロックを供給する。
BUSCNTL	3 ステートバス制御モジュール	モジュール内部でデータの調停を行う。
ADCIF	ADC インタフェースモジュール	ADC の制御を行う。
DACIF	DAC インタフェースモジュール	DAC の制御を行う。
DPMIF	デジタルポテンショメータ インタフェースモジュール	デジタルポテンショメータの制御を行う。
WRGEN	論理演算ブロック	主にデコードなどを行うブロック
CTRLREG	制御レジスタを保有する モジュール	アラームなどシステム関連のレジスタを 管理する

## 2) メモリ回路

メモリ回路は、その用途に応じて使い分けるため 3 種類のメモリを利用した。メモリは、主として FPGA 回路を仲介してマイコンと信号の送受を行い、制御アルゴリズムを実行する。更に、電源投入後およびリセット解除後に行うブート制御の初期設定値の格納、アーキテクチャシーケンス時のワークエリアおよび自律制御によって採取した光送受信機の実験データデータの格納を行う。また、メモリ回路にはワークエリア用に SRAM を、データ格納用に FRASH メモリを、ブート用に EPROM を用いた。メモリ回路の詳細を 図 3.11 に示す。

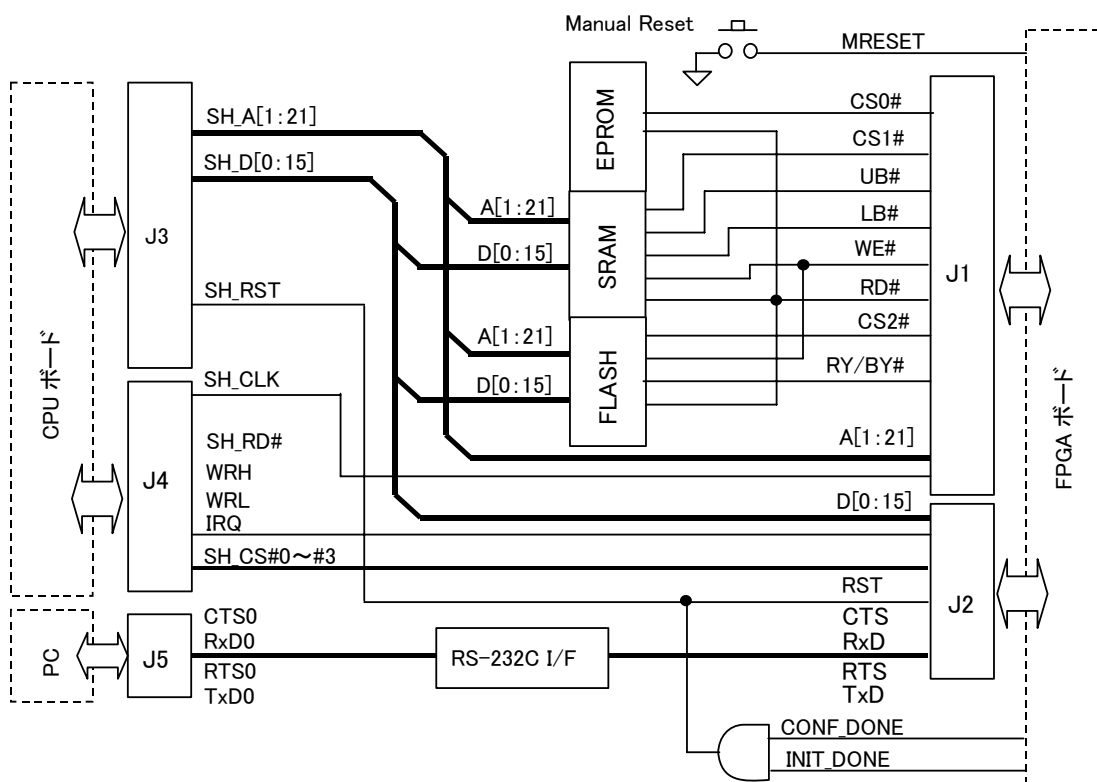


図 3.11 メモリ回路の構成



### 3. 3. 2 波長および光出力電力自動制御アルゴリズム

図 3.12 に高密度の WDM を実現するための波長および光出力電力を安定化させる光パワー調整を行う LD 駆動電流と波長の連動や LD の温度、光出力パワー、波長の関係を意識した自動制御アルゴリズムを示す。

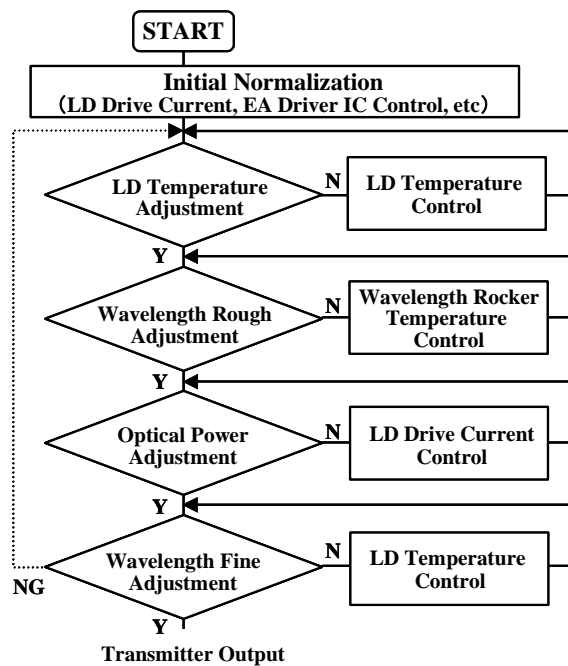


図 3.12 光送信機の波長および光出力電力制御アルゴリズム

#### (1) 初期設定

初期に光モジュール内蔵 LD の波長やそ温度係数、駆動電流、EA ドライバの信号振幅値、APC 回路の初期設定値、温度初期値、波長ロッカーのキャプチャレンジ等、自律に必要な基本となる項目を初期化する。光モジュール内の温度を、内蔵のペルチエ素子に流す電流の極性を反転させることにより、冷却あるいは加熱を行い、イニシャライズで設定した LD の所望値に収束させる。この時、モジュール内の温度は内蔵のサーミスタにてモニタリングする。

## (2) 波長の粗調整

光モジュール内の温度を所望値にした後に波長の粗調整を行う。波長制御フローでは、図 3.8 に示す波長ロッカー内の詳細を図 3.13 に示す。受光素子 PD1、PD2 に流れる電流を各々検出し、前置増幅器にて電圧  $V_{M1}$ 、 $V_{M2}$  に変換する。ここで、LD の温度が変動して出力光の波長が変動すると二つの電圧比率  $V_{M2}/V_{M1}$  が変化する。従って、電圧比率の初期値からの変動分を検出して、LD の温度に負帰還制御を掛けることにより、インシャライズで設定した所望の波長に収束させることができる。

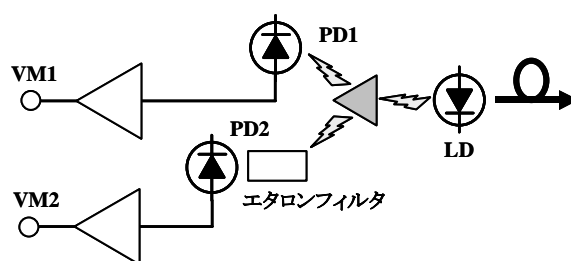


図 3.13 波長ロッカー

## (3) 光出力電力調整

LD の温度制御により光出力電力が変動するが、二つの電圧比率  $V_{M2}/V_{M1}$  は一定な値を示す。しかし、それらの絶対値は変動するので、光出力電力のモニタとして  $V_{M1}$  を用い、所望値からの変動分を検出して LD の駆動電流に負帰還し光出力電力制御を行う。

## (4) 波長の微調整

光出力電力を制御する場合、LD に流す電流値が増減するため、LD 内の温度が上昇、或いは、下降するので波長が若干シフトする。それ故、波長の微調整が必要となる。波長制御フローは (2) 項と同様に、電圧比率の粗調整値からの変動分を検出して、LD の温度に負帰還制御を掛けることにより、所望の波長に設定することができる。

### 3. 3. 3 波長検出

波長検出には、光透過波長特性に周期性があるエタロンフィルタを利用し、波長がシフトした場合の透過光量の変動を検出して波長補正する方法を用いた。ここで考慮すべ

きことは、LD の光出力電力の変動である。PD2 が検出する光モニタ電流は波長のずれから生じる変動だけでなく LD 自体の変動も感知するので区別することが困難となる。そこで、分岐された直接光をモニタ PD1 で受信し、その検出結果に変動が生じた場合は LD 自体の光出力電力変動とした。また、PD1 の検出結果に変動が無く、PD2 の検出結果のみが変動している場合を波長シフトと定義し、LD 温度を制御することにより変動量の補正を行った。但し、エタロンフィルタ自体が持つ波長-透過損失特性の温度依存性と LD の偏波状態に依存する透過特性の変動を考慮する必要がある。

### 3. 3. 4 エタロンフィルタの温度依存性の補正方法

エタロンフィルタの波長-透過特性に対する温度依存性を補正する係数を求めるための手法を検討した。図 3.8 において、LD、EA 変調器を恒温槽内に収納し、LD の温度が一定になるようペルチェ素子を制御し、LD 出力光の波長を固定する。次に、恒温槽の温度を変化させ、エタロンフィルタを透過した光量の変動分を PD2 の出力結果から検出する。この時、設定温度は一定に保たれているので、LD 波長変動は起こらずエタロンフィルタ固有の特性変動のみが検出できる。また、この変動値には LD 以外で起こる偏波特性の変動による劣化分も含まれるが、同時に補正できる。最後に、以上の検出結果をテーブル化し、波長ロック条件の補正係数とした。

### 3. 3. 5 LD の波長制御精度

使用したエタロンフィルタの透過光量の波長依存性は約 0.02dB/pm であった。波長と周波数の関係は、波長( $\lambda$ ) = 光速( $c$ ) / 周波数( $f$ )で与えられるから、例えば、 $\lambda = 1548.64\text{nm}$  とすると、 $f = c/\lambda = 193584.344\text{GHz}$  (ITU-T スペック) となる。従って、 $\Delta f_{\text{ITU}} = \pm 3\text{GHz}$  とすると、波長の変動量は以下ようになる。

$$\lambda = 1548.62 \sim 1548.66\text{nm} \quad (f = 193587.344 \sim 193581.344\text{GHz}) \quad (1)$$

以上の結果から、波長変動量  $\Delta \lambda_{\text{ITU}}$  を中心波長 1548.64 nm に対し  $\pm 20\text{pm}$  以下に抑える必要があることが分かる。これはエタロンフィルタの透過光量の波長依存性から計算すると約  $\pm 0.4\text{dB}$  の光出力電力の変動量に相当するが、10 倍以上の光出力電力制御ループの利得を得ることは容易であるので、光出力変動を  $\pm 0.1\text{dB}$  以下に抑えることは可能であ

る。これを波長制御精度に換算すると $\pm 2\text{pm}$ 以下となる。

### 3. 3. 6 LD の温度制御精度

一般に、実用的な光 WDM 伝送用 LD では波長を安定に出力させ得る動作温度範囲は $20\sim 30^\circ\text{C}$ 、波長変動量は $\pm 2\text{pm}$ 程度である。従って、 $\pm 10^\circ\text{C}$ の温度マージンを考慮しても LD の動作温度範囲は $10\sim 40^\circ\text{C}$ 程度である。それ故、8ビットの A/D 変換器にて温度制御をする場合には $0.12^\circ\text{C}/\text{ステップ}$ となり、十分制御可能な精度となる。

### 3. 3. 7 光伝送特性の最適化手法

光送信機の光出力波形は 10G-Ethernet や OC-192 等の標準規格であるアイマスク規定に収まるよう調整する必要がある。図 3.14 に光オシロスコープと光送信機を連動させ光出力波形の最適化を行う手法を示す。光送信機の出力信号情報を光オシロスコープで取込み、規格アイマスクに収まるよう、波長、消光比および光出力電力の規定値を維持しながら EA 変調器のバイアス電流、信号出力光の振幅およびクロスポイントの自動最適化が行われる。

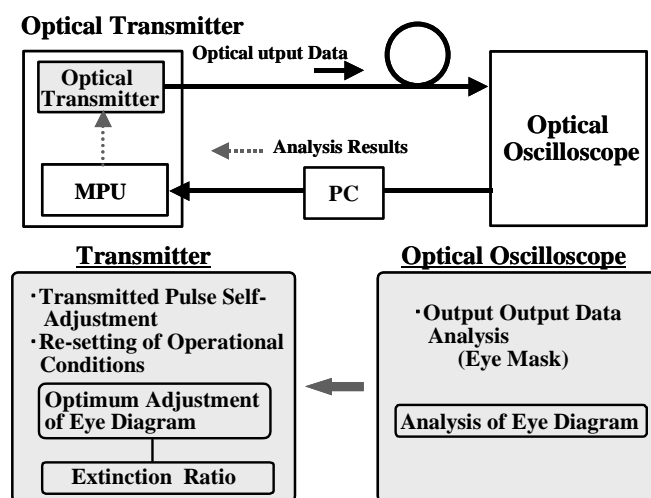


図 3.14 光伝送波形の最適化手法

### 3. 4 新アーキテクチャの検証実験結果と考察

新アーキテクチャの実現の可能性を確認するため、図 3.15 に示すブレッドボード実験用光送受信機を試作した。また図 3.16 にシステム全体の実験系を示す。実験機にはオンボードプログラミングが可能な FLASH-ROM を内蔵するマイクロプロセッサを搭載し、温度制御特性、光出力電力制御特性および波長制御特性の 3 点を中心とした自動制御アルゴリズムの検証を行った。10Gbit/s 光 WDM 伝送を可能とするため、光源には DFB-LD モジュールを用い、EA 変調器にてその出力光を変調する、外部変調方式を採用した。

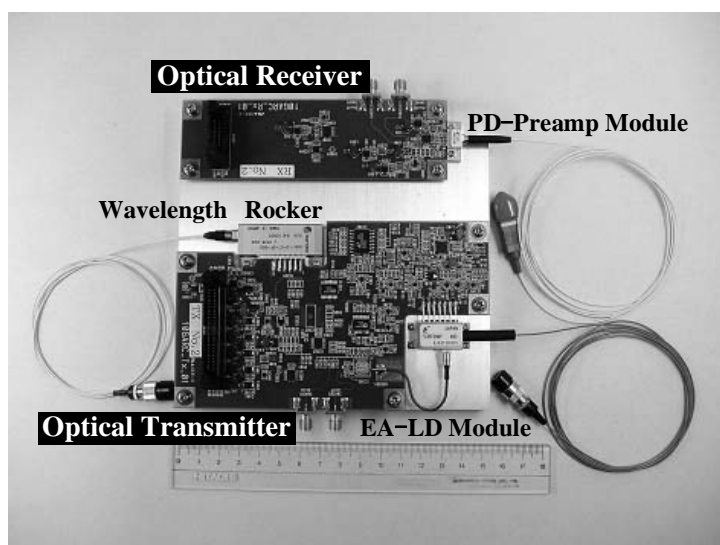


図 3.15 アーキテクチャ検証用光送受信実験機

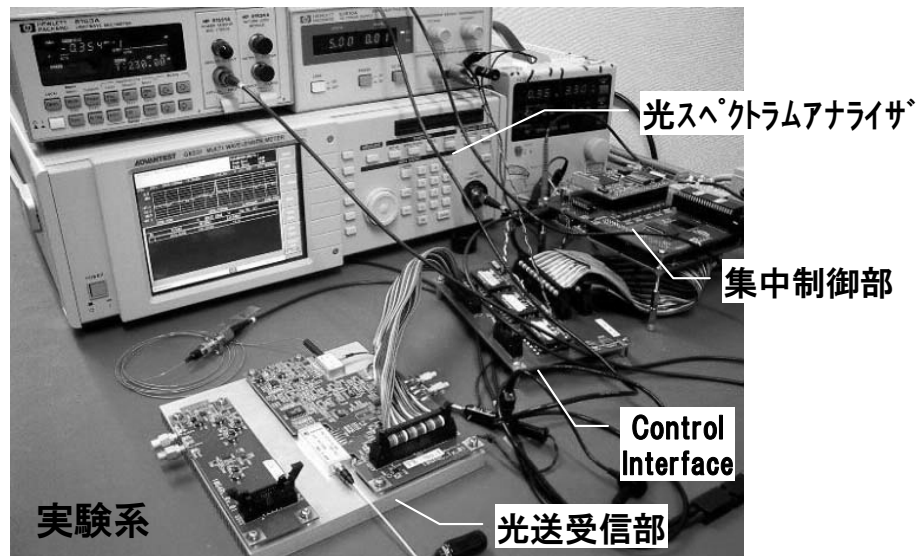


図 3.16 ブレッドボード試作実験の測定系

### 3. 4. 1 波長制御

#### a) 波長変動モニタ

DFB-LD の波長制御には、LD モジュール内蔵のペルチエ素子により DFB-LD を直接温度制御して所望の波長に固定する制御方式と波長モニタとしてエタロンフィルタの透過特性を利用した 2 受光レベル比検出方式を適用した波長ロッカーを併用した。エタロンフィルタには、その透過周期が ITU グリッド間隔 100GHz に対して 80GHz のものを使用した。図 3.17 に波長ロッカー用モニタ回路の構成を示す。LD のモニタ光は 2 分割され直接受光する PD1 とエタロンフィルタを透過させた後に受光する PD2 の 2 系統で検出する。

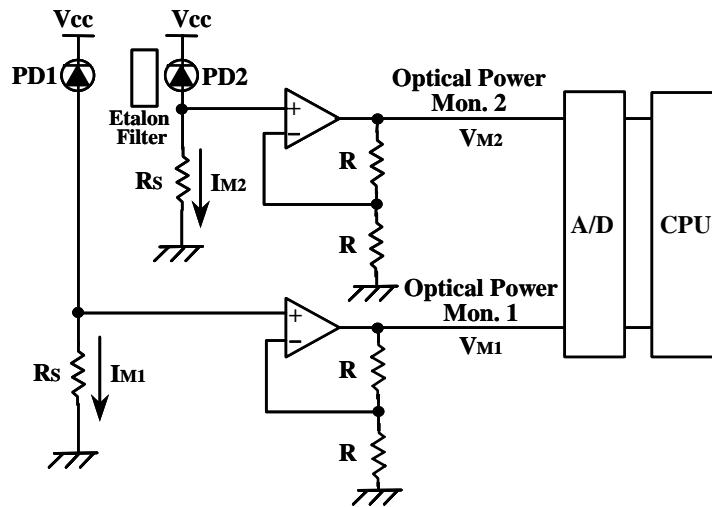


図 3.17 波長ロッカー用モニタ回路の構成

実験機に用いたDFB-LD 出力光波長の温度変動は高温で長波長側、低温で短波長側へシフトし、その変動量は約  $37\text{pm}/^\circ\text{C}$  であった。図 3.18 に波長モニタ用PD1 およびPD2 の検出光電流 $I_{M1}$ 、 $I_{M2}$  を電圧に夫々変換した $V_{M1}$ 、 $V_{M2}$  の温度依存性を示す。 $V_{M1}$ の変動はLD の温度変化による光出力電力変動分であり、 $V_{M2}$  の変動には光出力電力変動分と光波長変動によるエタロンフィルタの透過特性分が加算されたものとなるため、これら $V_{M1}$  および $V_{M2}$  の比が波長変動分を表す。従って、 $V_{M1}$  を基準値として $V_{M2}$ との比を検出し、その値が常に一定になるようにLDの温度を制御すれば、波長を任意の値に固定することができる。実際の波長変動の検出には、 $V_{M1}$  および $V_{M2}$  の比を差分信号 (dB) として取出すため、対数演算機能を内蔵するAD 変換器を用いた。この差分信号はMPU を介して制御信号として出力される。今回は、標準光出力電力におけるモニタPD の出力電流を $I_{M1} = 0.2\sim 0.6\text{mA}$ 、 $I_{M2} = 0.2\sim 0.6\text{mA}$  に設定した。検出電流範囲は部品の性能ばらつき等を考慮して  $0\sim 2.5\text{mA}$  とし、MPU 内蔵の 10 ビットA/D 変換器を利用した。この時の 1 ステップ当りの検出電流  $\Delta I_M$  は  $2.44\ \mu\text{A}$  となる。

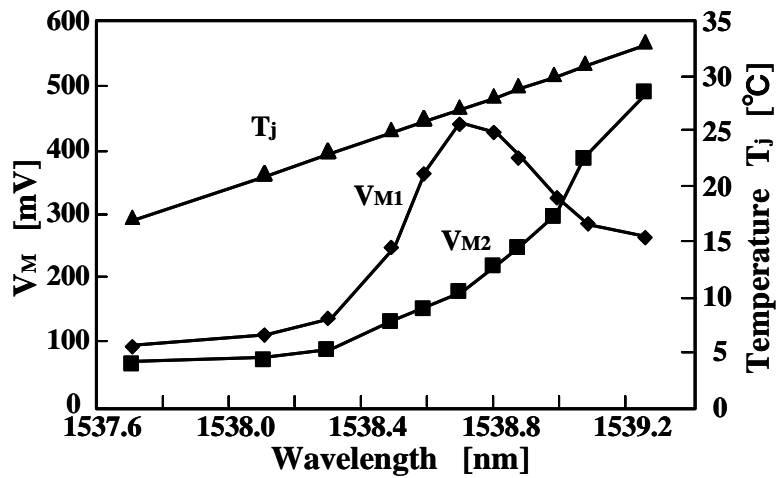


図 3.18 モニタ PD1、PD2 の検出光電流温度依存

b) 波長の電流依存性

光出力電力の安定化にはPD1 のモニタ光電流 $I_{M1}$ を常時監視し、 $I_{M1}$  が一定になるようLD の駆動電流を制御した。しかし、LD の出力光波長はLD に流す駆動電流にも依存するため、波長 1548.14nm、1547.76nm、1547.88nm の3サンプルにおける波長のLD 駆動電流依存性を評価した。これらの結果から、波長変動量は約 6.4pm/mA であり、サンプル間の相異は小さかった。一方、設計目標の動作温度範囲 10~40 °Cにおいて光出力電力を一定値に保つのに 20mA程度の電流制御が必要となる。従って、10~40 °Cの温度範囲では約 130pm の波長変動が生じることになる。しかし、この変動量はLD 温度を一定にして波長を安定化させるATC 方式を用いているため、実際にはこの変動量を抑圧可能で、ITU-T 規格のグリッド間隔 10.8nm (100GHz グリッド) を十分に満足できる。

d) 波長制御動作の安定性

波長制御動作の初期におけるペルチェ素子の温度は、帰還ループの収束性を考慮して波長ロック近傍の温度に設定し、1分間この状態を保持させて初期温度の安定化を図った。次に、PD1、PD2 の検出結果を基にペルチェ素子に流す電流を変化させて、LD の温度を制御し、波長を所望値にロックさせた。波長の制御精度は制御電圧幅と MPU 内蔵のD/A 変換器の分解能 (ビット数) で決定される。図 3.19 にペルチェ素子温度制御回路の構成を示す。ペルチェ素子制御用のバッファ回路は、前段にオペアンプを置くことに



より電流駆動用 FET の  $V_{gs}$  (ゲート・ソース間電圧) バラツキを吸収してクロスオーバー歪が発生しないような回路構成となっている。

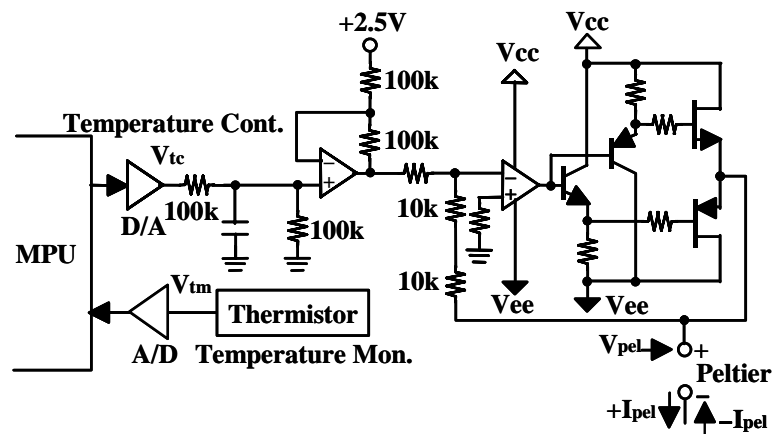


図 3.19 ペルチエ温度制御回路

図 3.19 より、ペルチエ素子の制御電圧  $V_{pel}$  は次式で与えられる。

$$V_{pel} = -V_{tc} + 2.5(V) \quad (2)$$

$V_{tc}$  の範囲は  $0 \sim 5V$  であるので、 $V_{pel} = -2.5 \sim 2.5V$  となり、 $-1 \sim +1[A]$  のペルチエ素子電流制御が可能となる。制御用 D/A 変換器には 10 ビットの精度 (分解能) を持つ MPU 内蔵のものを用いた。制御電圧を  $\pm 2.5V$  の範囲で 1 ステップ当りの制御電圧および電流は  $\Delta V_{pe} = 4.88mV$ 、 $\Delta I_{pel} = 1.95mA$  となる。

c) 波長制御検証実験結果

以上の検討結果を基に試作実験を行い、波長制御アルゴリズムの検証を行った。図 3.20 に、定常動作時における試作光送信機の周囲温度に対する波長依存性を示す。波長変動量は  $10 \sim 40 \text{ }^\circ\text{C}$  の温度範囲において  $2pm$  以下であった。図 3.21 は周囲温度を約  $1 \text{ }^\circ\text{C}/\text{分}$

で時間掃引した時の波長の安定性を示したもので、4pm 以下の波長制御が可能であることが分かった。これらの結果から、自動制御系が十分な機能を果たしていることを確認できた。

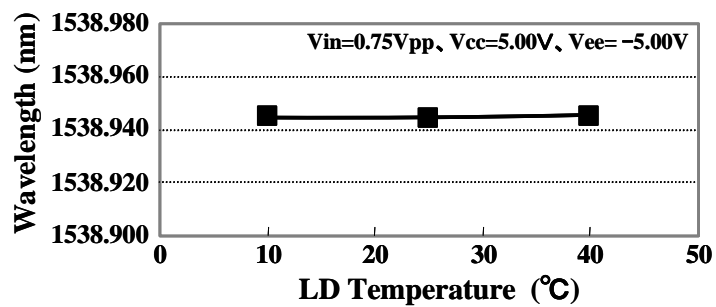


図 3.20 波長の周囲温度依存性

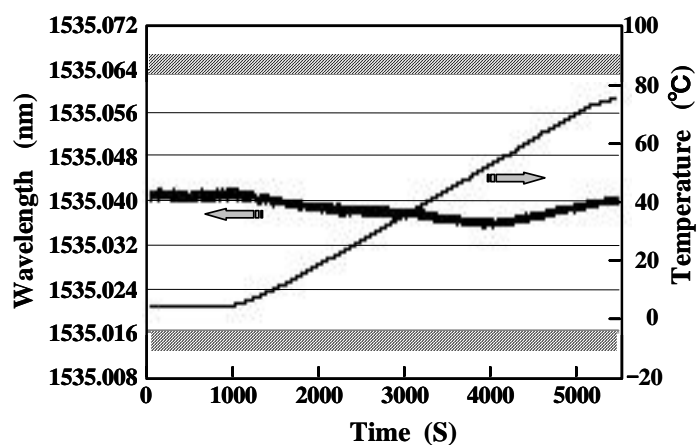


図 3.21 初期調整終了後における光出力電力の温度特性

## 光出力電力制御

### a) 光出力電力の制御精度

光送信機には、その光出力電力を一定に保つことが要求される。しかし、LD は温度に対して閾電流および外部微分量子効率の変動が大きく、これらの影響による光出力変動を補償する必要がある。また、経年劣化の補償も必要となる。この光出力電力の安定化には、PD1 のモニタ光電流 $I_{M1}$  を監視し、この値が常に一定になるようLD の駆動電流を制御して安定化を図る。光出力電力の変動分は波長制御と並行してAPCループを介しLDの駆動電流を制御することにより抑圧できる。図 3.22 にAPC 回路の構成を示す。ここで、MPU 内蔵の 10 ビットD/A 変換器を使用し、制御電圧の範囲を 0~5V、抵抗 $R_E$  を 10  $\Omega$  とすると駆動電流の制御分解能  $\Delta I_{LD}$ 、 $\Delta V_{LD}$  は夫々4.88mV、488  $\mu$  A となる。

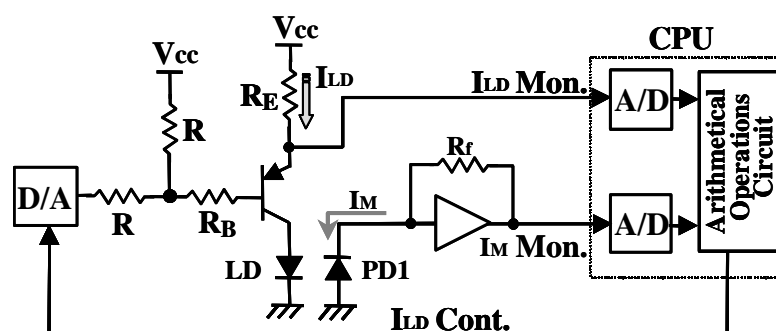


図 3.22 APC 回路の構成

### b) 光出力電力制御検証実験結果

以上の結果を基に試作実験を行い、光出力電力制御アルゴリズムの検証を行った。図 3.23 に定常動作時における光出力電力の温度依存性を示す。周囲温度範囲 5~75  $^{\circ}$ C における光出力電力の変動量は 1dBm  $\pm$ 0.2dB であり、ITU 規格の許容範囲を十分満たすことを確認できた。

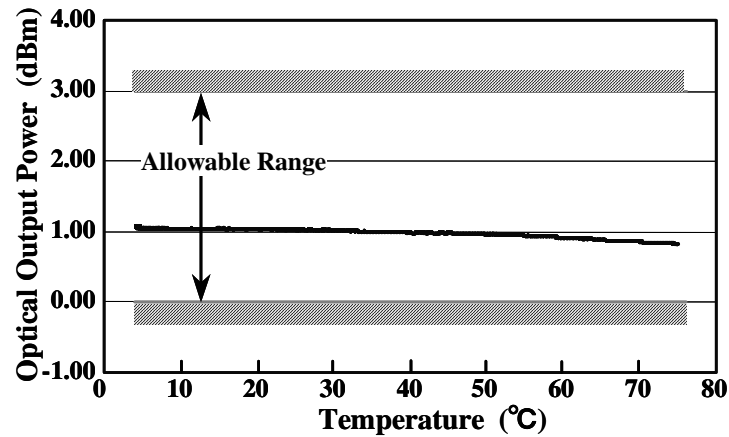


図 3.23 初期調整終了後における光出力電力の温度特性

### 3. 4. 2 波長および光出力電力制御総合検証実験結果

以上の基礎検討結果を基に、制御アーキテクチャの総合検証実験を行った。

図 3.24 に、自動制御時間に対する光出力電力、波長、温度およびバイアス電流の各モニタ値の時間変動を示す。制御動作は、送信機が送信動作開始時に行うシャットダウン (SD) 機能解除後に、光出力電力モニタ較正 (a)、波長粗調整 (b)、光出力電力調整 (c)、波長微調整 (d) の順で行なわれており、正常に自動制御ができていることを確認できた。SD 解除後、波長および光出力電力調整が完了するまでの全時間は 360 秒であり、新アーキテクチャが調整時間の短縮に有効であることを検証できた。

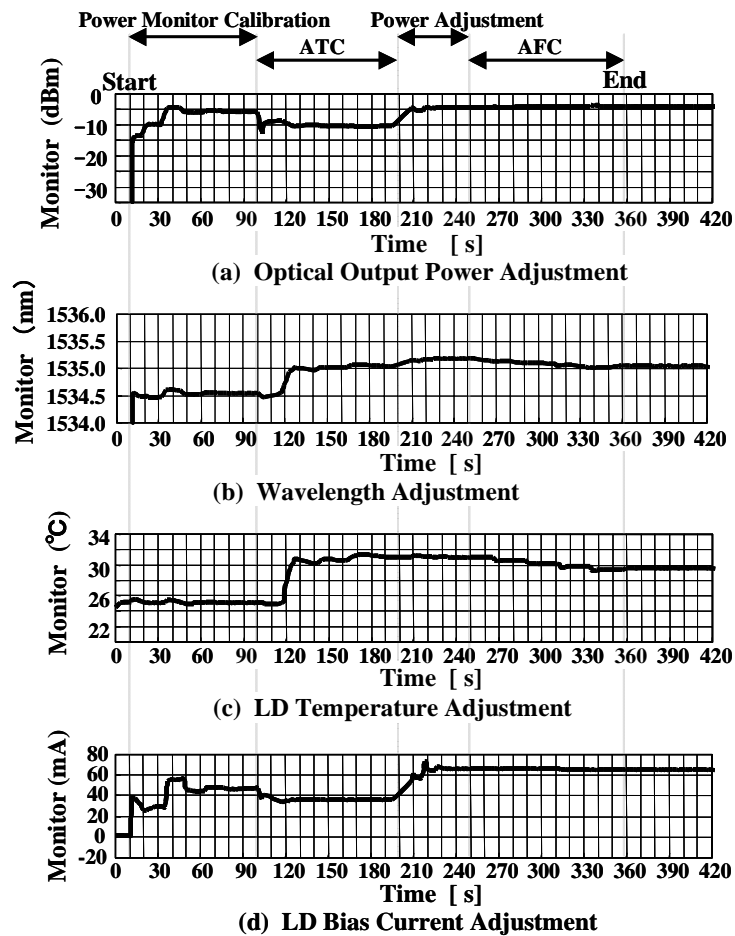


図 3.24 新アーキテクチャの総合検証実験結果

### 3. 4. 3 光出力波形制御

光送受信機の光出力波形の最適化に関する検証実験を行なった。今回の検証実験では、光オシロスコープを用いて波形データを取得し、外部接続の PC を光送受信機内蔵の MPU と連動させることにより波形データを光送信機にをフィードバックした。光送信機ではそれら情報を基に光送信パルスのクロスポイントや消光比の最適化を自律的に行った。図 3.25 に試作光送信機の 10Gbit/s 出力アイパターンを示す。10～40 °C の温度範囲で 10Gbit/s (OC192) 規格のアイマスクを満足しており、良好なアイ開口度を得ることができた。また、各温度における光波形の劣化は殆んど見られなかった

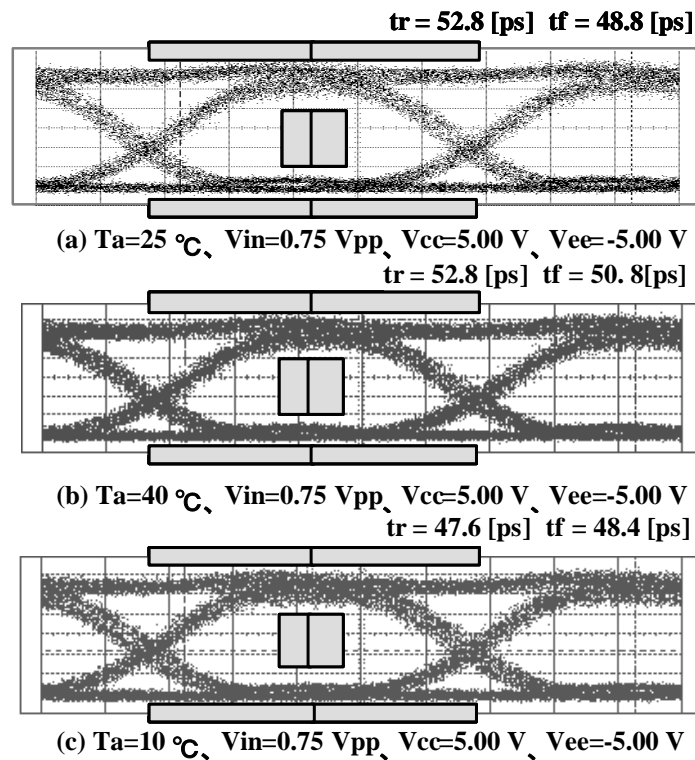


図 3.25 光送信機の実出力波形 (H:20 ps/div、V:200  $\mu$  W/div)

### 3. 5 自律制御アーキテクチャのシミュレーションによる検討

#### 3. 5. 1 シミュレータ

提案した自律制御インテリジェントアーキテクチャの有効性を短期間で検証するため、SPICE系シミュレータを利用して、光出力制御ループおよび光波長制御ループの応答特性を解析する簡易型電気シミュレータを開発した。その結果、ループの応答特性のみならず、光デバイスの製造バラツキや温度特性の許容範囲、ループ制御に用いる A/D および D/A 変換器の最適サンプリング周波数の明確化が可能となり、ループ応答の高速化手法の考案にも適応できた。本項では、光出力制御ループの応答特性の解析結果を中心に述べる。なお、光波長制御ループに関しては光出力制御ループと同様の結果が得られている。

### 3. 5. 2 光出力制御ループのモデル化

図 3.26、図 3.27 に光出力制御ループのブロック構成および電気シミュレーション回路図を示す。図 3.26 は微量量子効率  $\eta$  のブロックを介して電流  $I_b$  により光出力  $P_o$  が出射される LD 光源を表わしたもので、 $\beta$  はモニタ用 PD との光結合係数を表わす。また、 $\alpha$  は PD の光 - 電流変換係数、 $G_{IV}$  は電流 - 電圧変換係数、 $G_{VI}$  は電圧 - 電流変換係数、 $V_r$  は基準電圧であり、 $I_s$ 、 $I_{th}$  はそれぞれ信号電流および閾値電流を表わす。図 3.27 における  $I_p$  は光出力を電源に置き換えたもので、 $I_{pn}$  はループ応答特性を解析に必要な擾乱電流である。なお、CR回路はペルチェ素子の温度応答特性を等価的に表したものである。

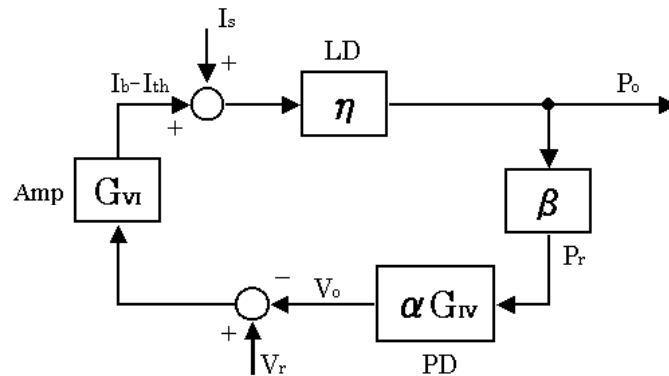


図 3.26 光出力制御ループのブロック構成

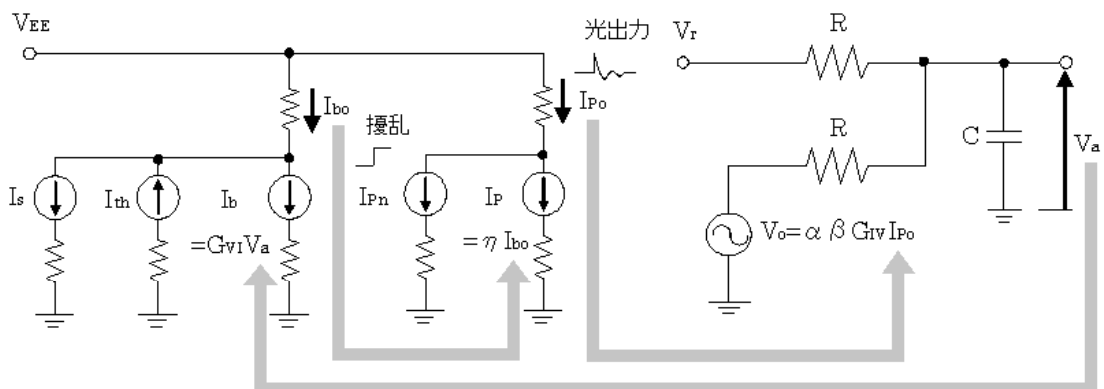


図 3.27 電気シミュレーション回路 (光出力制御)

### 3. 5. 3 シミュレーション結果および考察

今回は外部変調方式を採用するので信号電流 $I_s$ 制御は考えず、図 3.28 のシミュレーション回路を用いてループ応答特性の解析を行った。この時の一巡伝達関数は、A/DおよびD/A変換器のサンプリング周波数が非常に高いとすれば次式のようななるラプラス変換で表記できる。

$$W(s) = \frac{\eta G_{VI}}{1 + \frac{\alpha\beta\eta G}{1 + Ts}} \quad G = G_{VI}G_{IV} \quad (3)$$

この式より電流利得  $G$  を大きくすれば擾乱に対する収束誤差は小さくなり、 $G$  を大きく、或いは、時定数  $T$  を小さくすれば収束速度は速くなることが分かる。

図 3.28 は、微分量子効率  $\eta = 0.05 \text{mW/mA}$  を標準状態とした時のシミュレーション結果を示したもので、 $G$  を大きくすれば収束誤差を小さくできることを示す。図 3.29 より、光出力の変動許容量を  $\pm 0.3 \text{dB}$  とすれば、 $G=20000$  の時、微分量子効率は少なくとも  $0.02 \sim 0.08 \text{mW/mA}$  の範囲の製造バラツキを吸収することが可能だとわかる。図 3.29 に解析時間刻みが  $20 \mu \text{m}$  の時の過渡応答特性を示す。時定数  $T$  が短くすると応答特性に振動現象が現れるが、これは動作解析が離散的に行われることに起因する。

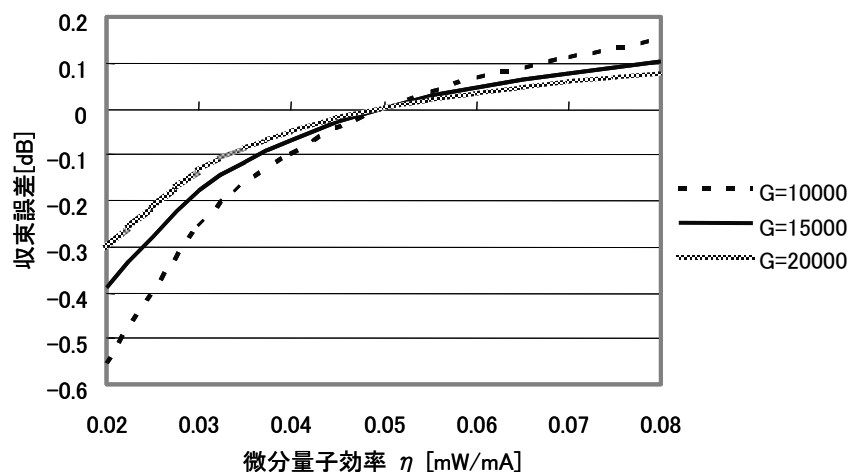


図 3.28 収束誤差（光出力制御ループ）



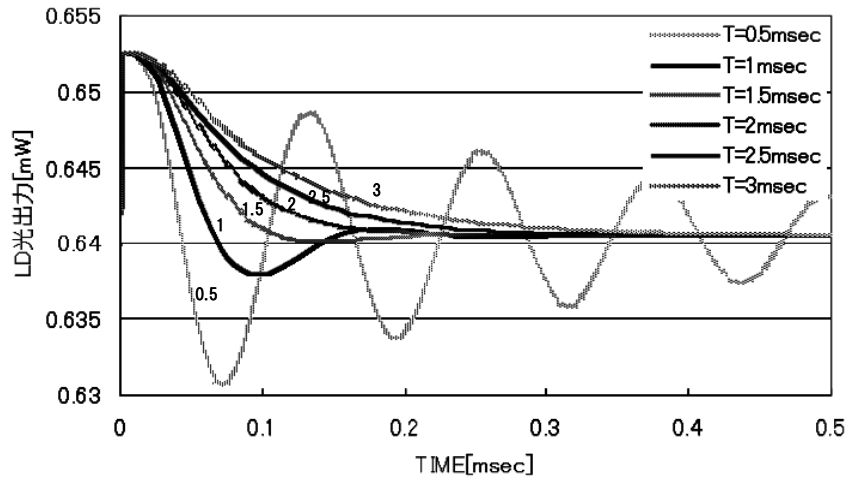


図 3.29 時定数変動時の過渡応答（光出力制御）

それ故、実際の回路では解析時間刻みを A/D および D/A 変換器のサンプリング周期に対応させることができるので、シミュレーション結果から A/D および D/A 変換器に要求されるサンプリング周波数と電流利得  $G$  の値を決める手立てとなる。図 3.30 に解析時間刻みと応答特性の関係を示す。解析時間刻みを  $5\mu\text{sec}$  以下にするとオーバーシュートおよびアンダーシュートが見られなくなる。即ち、サンプリング周波数  $200\text{kHz}$ （周期  $5\mu\text{sec}$ ）以上の A/D および D/A 変換器を使用すれば、安定した応答特性を得ることが可能となる。また、解析時間刻みを小さくすると、遅れ時間  $T_d$ （最終値の 50%に達するまでの時間）の短縮が可能となる。反面、解析時間刻みを短くし過ぎると立下り時間  $T_f$ （最終値の 10%~90%まで変化するのに要する時間）が長くなり、即応性が無くなる。以上の結果から、オーバーシュートが 10%以下で立下り時間  $T_f$  が最小となる値  $8\mu\text{sec}$ （A/D および D/A 変換器サンプリング周波数： $125\text{kHz}$ ）が最適であることが分かった。この時の収束応答時間は  $0.058\text{msec}$  である。

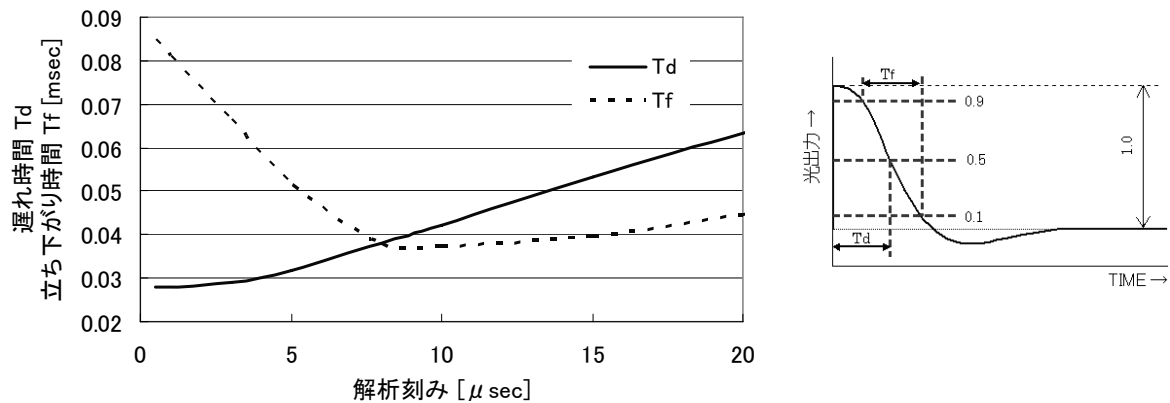


図 3.30 解析刻み時間に対する過渡応答の遅れ時間変化及び立上り時間変化

### 3. 5. 4 ループ応答の高速化

実際の回路の時定数はペルチェ素子の温度時定数で決まるので、収束速度を高速化するための方法として、新たに高域補償回路方式を導入した。シミュレーションに用いた遅延回路および補償回路を図 3.31 に示す。この 2 つの回路を接続した時の伝達関数は、以下の式で表される。

$$\begin{aligned}
 G(s) &= \frac{V1}{V2'} = \frac{V1}{V2} \times \frac{V1'}{V2'} \\
 &= \frac{1}{1+T_1s} \times \phi \frac{R2}{R1+R2} \frac{1+T_1s}{1+T_2s} \\
 &= \phi \frac{R2}{R1+R2} \frac{1}{1+T_2s}
 \end{aligned}
 \quad \left. \vphantom{\begin{aligned} G(s) &= \frac{V1}{V2'} = \frac{V1}{V2} \times \frac{V1'}{V2'} \\ &= \frac{1}{1+T_1s} \times \phi \frac{R2}{R1+R2} \frac{1+T_1s}{1+T_2s} \\ &= \phi \frac{R2}{R1+R2} \frac{1}{1+T_2s} \end{aligned}} \right\} (4)$$

ここで、 $V1' = \phi V2$ 、 $T_2 = CR1 \parallel R2$  である。式 (2) より、 $T_2$  を小さくする、即ち、 $R2$  を小さくすれば収束速度が速くなるのが分かる。図 3.32 に  $G$  を 15000、 $T_1$  を 4msec、解析時間刻みを  $10 \mu \text{ sec}$  とした時の  $R2$  に対する過渡応答特性を示す。この時の  $R1$  は  $1k\Omega$  とした。同図より、補償回路を挿入することにより収束速度が速くなるのが分かる。また、 $R2$  を小さくするほど収束は速くなるが、小さくし過ぎると、前述した様に振動的な応答特

性を呈し収束時間が長くなる。よって、この条件では、オーバーシュートが 10%以下でR2の最も小さい 800Ω、即ち、高域補償回路の時定数を 1.78msecとした時が最適であり、収束時間は 0.319msecから 0.106msecとなるので、補償回路の無いときに比べて約 3 倍の高速化を実現できる。これらのシミュレーション結果より、実際に光出力制御を行う時には回路時定数、電流増幅度、解析刻み時間（A/DおよびD/A変換器のサンプリング周波数に相当）、高域補償回路などを考慮すれば、光出力変動の収束時間を短かくできることが分かった。

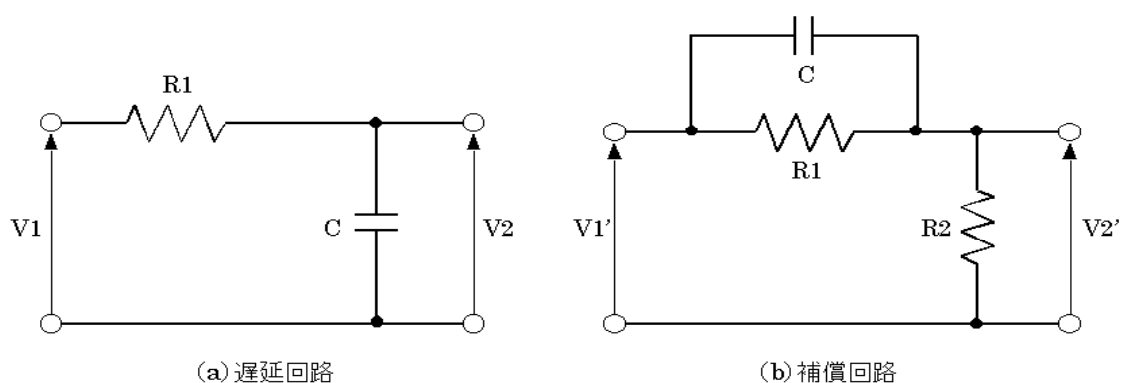


図 3.31 遅延回路および補償回路

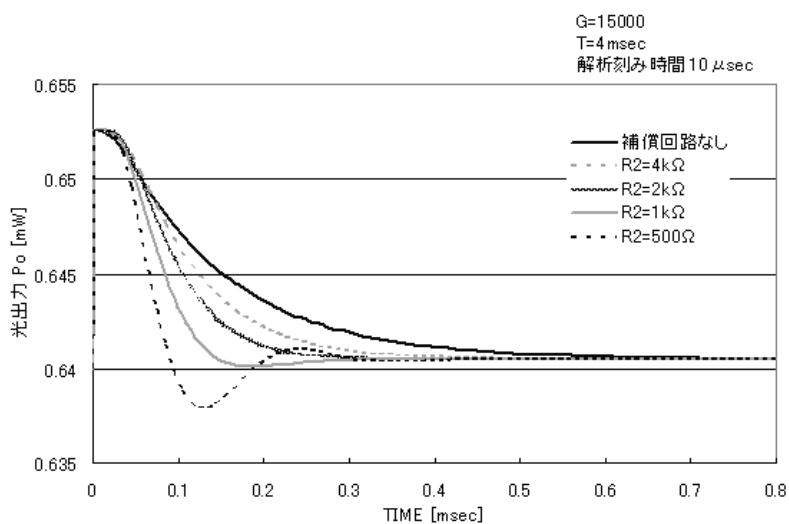


図 3.32 補償回路挿入時の過渡応答（光出力制御）

### 3. 5. 5 光波長制御ループのシミュレーション解析結果

シミュレーション解析では、エタロンフィルタの光波長透過特性を一次近似し、1549.9～1550.3nm の波長変動（温度変動 10°C）で収束誤差 0.017nm 以内、収束時間は時定数  $T=1\sim 4\text{msec}$  の時、0.09～0.35msec あった。 $T=1\text{msec}$  の時、解析時間刻みを  $5\mu\text{sec}$  以下にすると解析時間刻みの影響が無くなるが、解析時間刻みが  $8\mu\text{sec}$  の時最も速く収束する。これは A/D および D/A 変換器サンプリング周波数に換算すると 125kHz に相当する。また、回路時定数 4msec の場合に最も速く収束するのは時定数 1.78msec の補償回路を挿入した時で、収束時間は 0.335msec から 0.104msec に短縮され、補償回路が無い時に比べて約 3 倍速く収束する。なお、光波長制御ループでは LD の温度制御が行われる。その温度の変化分を光出力制御ループの および に反映させれば、LD 光源の自律制御が可能となる。

### 3. 6 システム LSI の方式および要素回路の開発

本章では、前章で述べたインテリジェントアーキテクチャを具現化するシステム LSI の開発に向け LSI 化の観点から構成と方式の検討を行う。また、検討結果から得られた開発課題を整理し、それを解決するための要素回路技術を提案する。最後にその有効性を実証するための要素回路 TEG (Test Element Group) の試作結果について述べる。

#### 3. 6. 1 システム LSI の構成と開発課題

本研究のシステム LSI の基本構成を図 3.33 に示す。本 LSI は MUX (Multiplexer)、DEMUX (Demultiplexer)、光部品の駆動条件をインテリジェントに制御する MPU (Micro Processing Unit) コア及び EA (Electronic Absorption) 変調器と波長ロッカーのアナログ信号のダイナミックレンジを調整する可変利得アンプからなる。MPU コアは A/D および D/A 変換器からなるアナログ I/O ポートを含む。MPU は EA 変調器から LD の出力光強度 (PD\_LD) を受け取り、出力が所望の値になるように LD の駆動電流 ( $I_{LD}$ ) を制御する。また、波長ロッカーからエタロンフィルタ通過前と通過後の光強度 (PD1, PD2) を受け取り、LD の出力波長が所望の値になるように LD の温度は、ペルチエ素子を使って制御する。この際、制御の補正データとして LD と波長ロッカーの温度 ( $T_{LD}$ ,  $T_{WL}$ ) を使用する。光波形の調整は、変調器駆動信号 ( $Tx_{out}$ ) のバイアス電位、振幅、クロスポイントを変化

させることで行う。また、MPU はピークディテクタを介して TXout のバイアス電位及び振幅を常にモニタしており、この情報も波形制御に使用される。制御プログラム及びデータは MPU コア内のフラッシュメモリに格納されており、必要に応じて内蔵 SRAM に読み込まれ使用される。

MUX 部は、XAUI インタフェース、エンコーダ、クロック通倍回路および 4:1 MUX からなる。4 本の 2.5Gbit/s の入力信号 (TXin[3:0]) は XAUI インタフェース回路 (XAUI) を通り、64B/6B および 8B/10B に符号化された後に 4:1 MUX で 10Gbit/s に多重化される。この際使用される 10GHz クロック信号は参照クロック (Ref. CLK) からクロック通倍回路により作られる。

DEMUX 部は入力信号 (Rxin) を一定振幅まで増幅する AGC アンプ、1:4 DEMUX、デコーダ、XAUI インタフェース及びクロック再生回路 (CR) からなる。10Gbit/s の入力信号 RXin は、AGC アンプで一定振幅まで増幅され、1:4 DEMUX によって 4 本の 2.5Gbit/s 信号に分離され、更に 64B/66B、8B/10B に復号化され、XAUI インタフェースを通して出力される。DEMUX で使用する 10GHz クロック信号は入力信号からクロック再生回路により再生される。

今回開発するシステム LSI は、市場におけるコスト優位性を確保するため、製造コストの低い 0.18  $\mu$  m CMOS 製造プロセス技術を用いて開発する。しかしながら、後述するように 0.18  $\mu$  m CMOS 製造技術は 10 Gbit/s システム LSI に適用するにはデバイス性能が不十分であり、従来の回路技術をそのまま使用しては 10 Gbit/s 動作は不可能である。そこで、デバイス性能の不足を補う回路技術の開発が必須となる。以下では、まずデバイス性能を極限まで引き出し 10 Gbit/s 動作を可能にするピーキング技術、チップ面積の大幅削減を可能にするハーフレート方式の導入及び小型、低消費電力 MUX/DEMUX 技術について述べる。

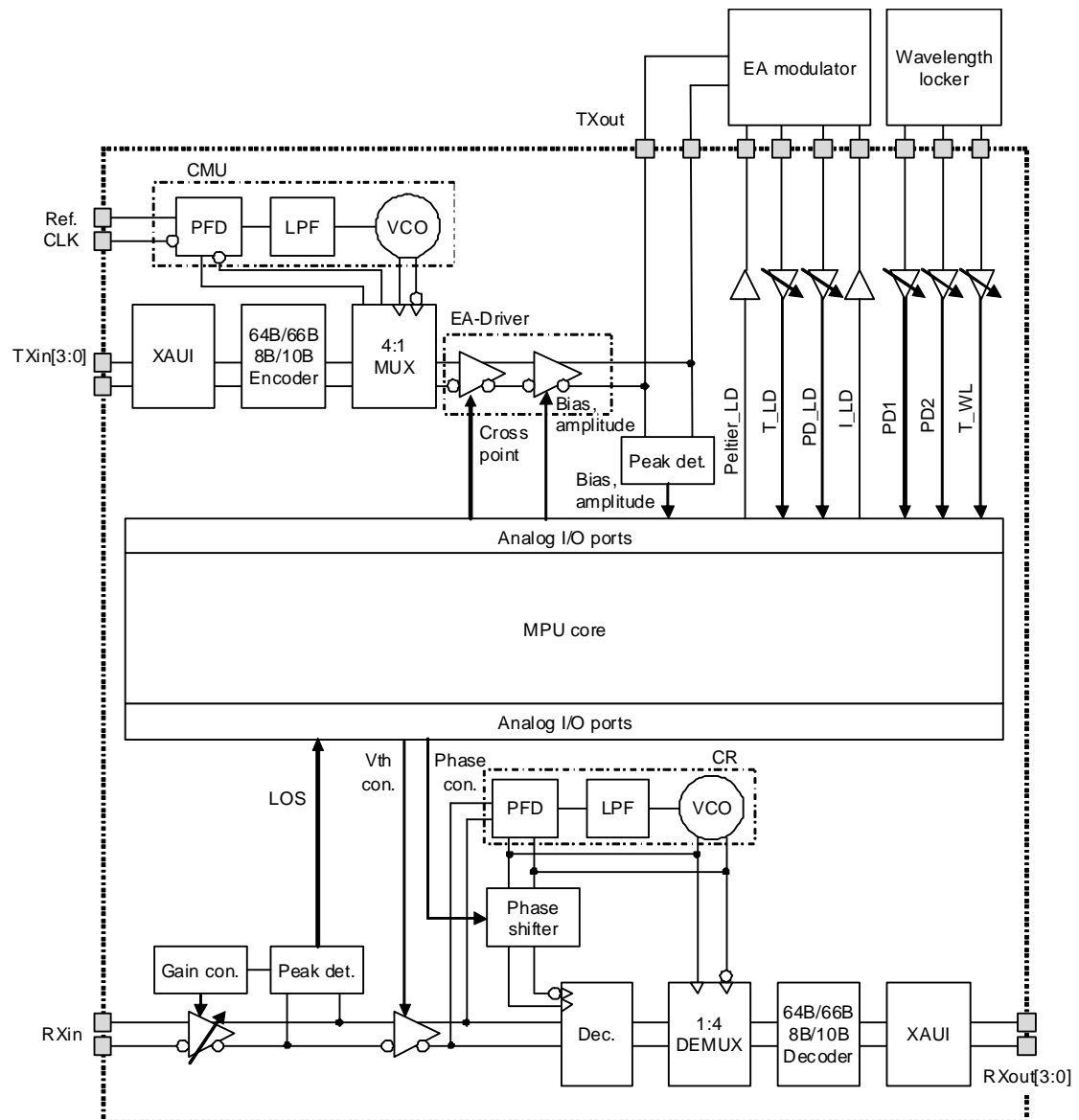


図 3.33 システム LSI の基本構成

### 3. 6. 2 EA-Driver 回路

EA 変調器を使用して良好な光波形を得るためには広帯域な駆動電気波形が必要不可欠である。0.18  $\mu\text{m}$  プロセスを使用して 10Gbit/s 動作の回路を構成した場合、通常回路では

帯域が不足するため、EA-Driverとして、何らかの帯域補償（高速化）技術を適用する必要がある。

図 3.34 は、シミュレーション設計に用いた  $0.18\mu\text{m}$  CMOS プロセスで構成した、通常の差動増幅器の回路図である。この回路での周波数特性を図 3.35、また入出力波形を図 3.36 に示す。回路シミュレーション時には寄生素子、次段の回路の影響を考慮している。シミュレーション結果から小信号での 3dB 帯域は、6GHz であり、また出力信号の立上り／立下り時間は 66ps／59ps となった。この結果は、EA-Driver として明らかに帯域が不足しており、10Gbit/s 伝送を可能とするためには、回路の広帯域化の改善が必要であることがわかる。

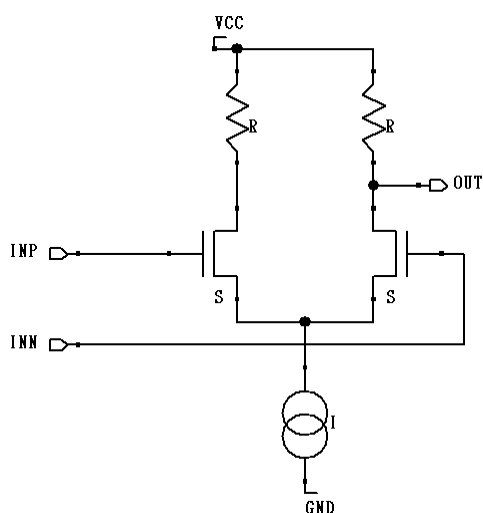


図 3.34 差動増幅器の回路構成

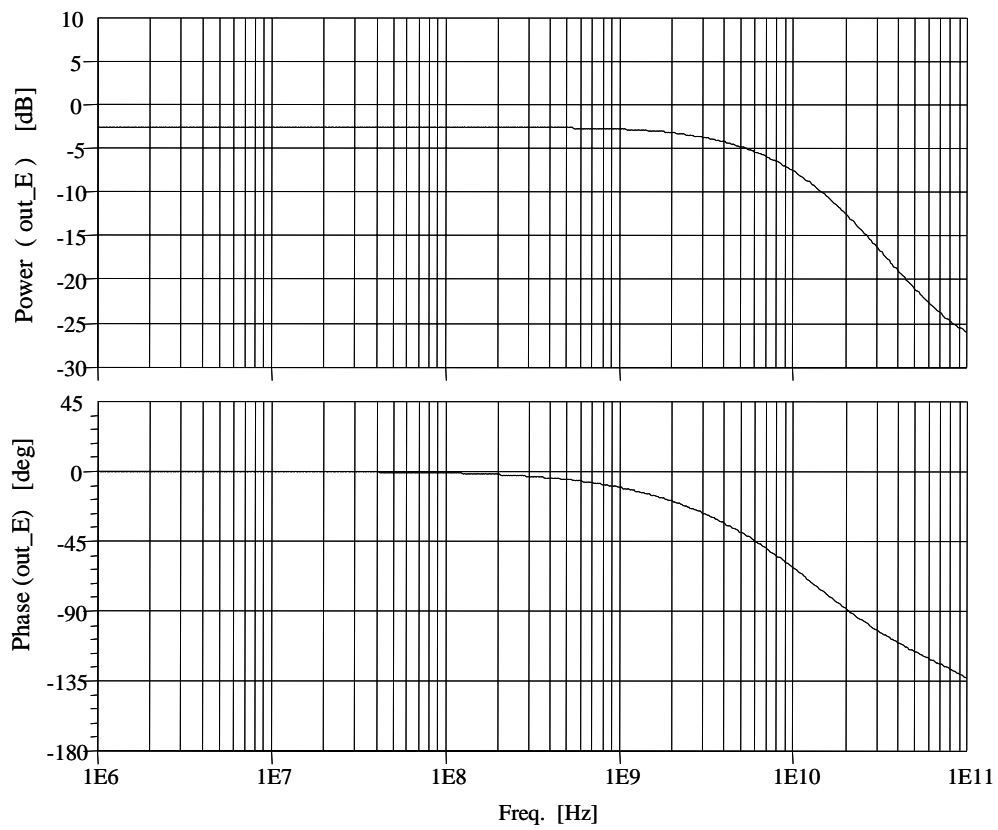


图 3.35 周波数特性

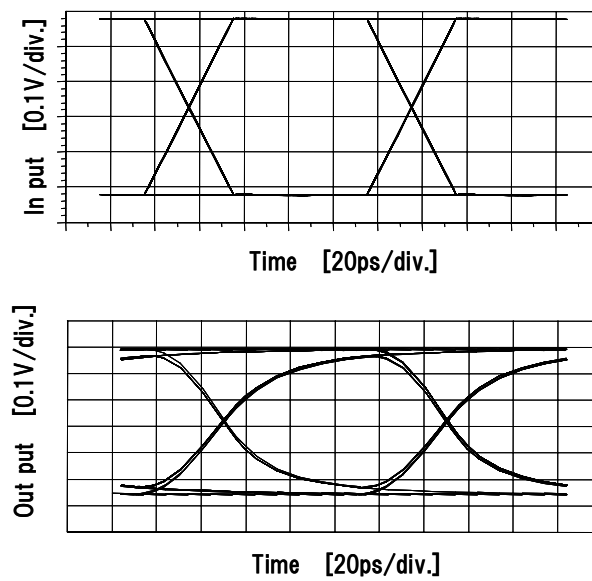


图 3.36 入出力波形



回路を高速化するためには以下の 2 つの方法がある。一つは、高速なプロセスを使用し、素子レベルで高速化する。もう一方は、高周波域で低下する利得を補償することができる高域通過特性を強調させる回路的に付加する手法（ピーキング）である。今回は研究の目的に沿い、プロセスは変更せず、後述のピーキングでの帯域補償による高速化を行った。10GHz クラスの回路構成では、回路を複雑にすると回路を構成する素子の寄生効果（寄生容量、寄生インダクタンス、寄生抵抗等）が大きく影響してくるため、逆に特性が劣化してしまう可能性が大きい。このため回路は、なるべくシンプルな構成が望ましい。以上を考慮して、高速化には回路構成が単純なインダクタピーキングを用いた。この回路は、差動対の負荷抵抗に直列にインダクタンスを接続することで、高周波動作領域での利得を補償し、回路の広帯域化を行う。

図 3.34 にインダクタピーキングを用いた差動増幅器の回路図を示す。また図 3.35 に小信号の周波数特性を、図 3.36 に回路の入出力波形を示す。帯域補償後のシミュレーション結果は、小信号 3dB 帯域が 11GHz、出力波形の立上り/立下り時間は、39ps/36ps となり 10Gbit/s 伝送に適応可能な見通しを得ることができた。

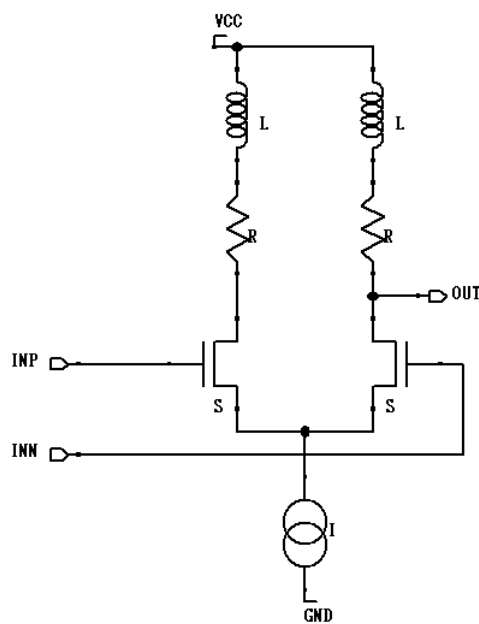


図 3.37 帯域補償後の差動回路

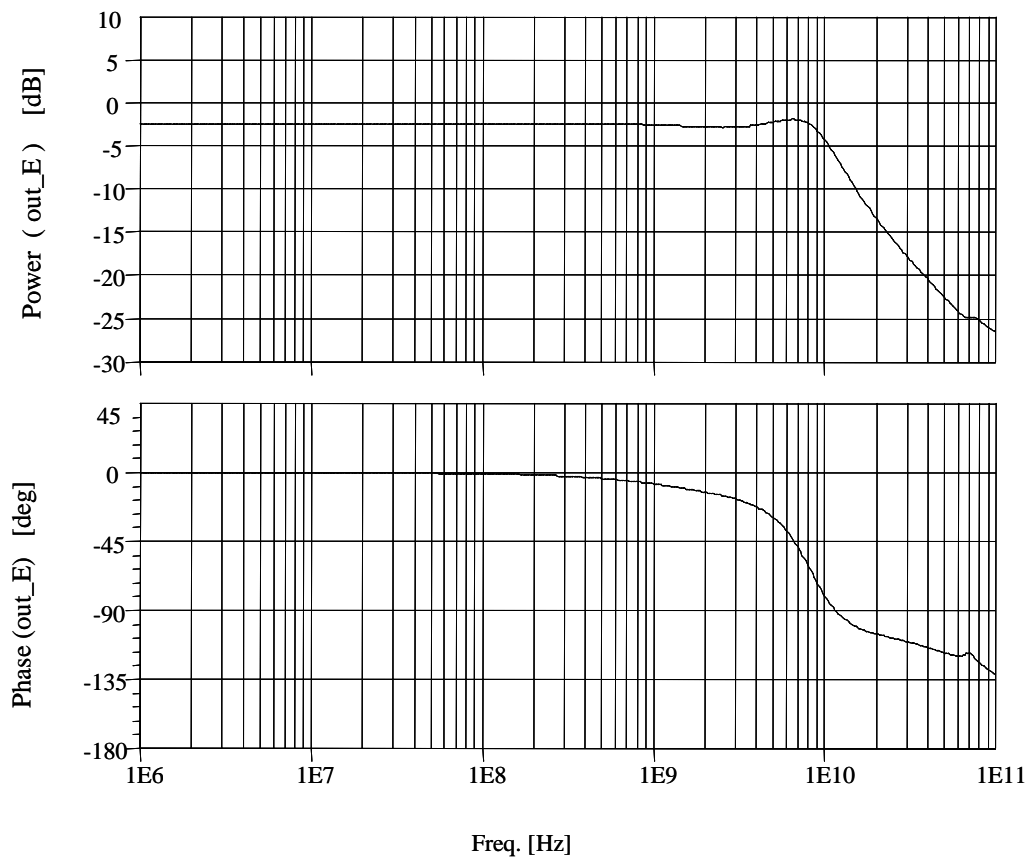


図 3.38 帯域補償後の周波数特性

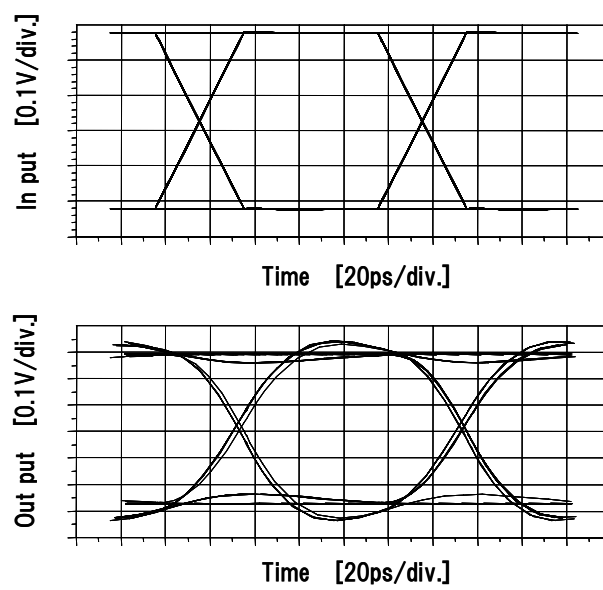


図 3.39 帯域補償後の入出力波形

### 3. 6. 3 分周器

0.18  $\mu\text{m}$  CMOSプロセスによる 10 Gbit/s動作実現の可能性を検証するため、本システムLSIの中でも最も高速動作が要求される 10 GHz分周器を例題に予備検討を行った。分周器は図 3.40 に示すように 2 つのD-FFで構成される。D-FFは高速性に優れたCML (Current Mode Logic) で構成した。VDD=1.8V、T=25°Cの条件下で回路シミュレーションを用いてこの回路の性能を予測したところ、図 3.41 のように回路の駆動電流を 3mAに設定することで 12 GHzまでの分周動作を確認できた。しかしながら、VDDを-10%、T=100°Cとした最悪環境条件下では最大分周周波数は 8GHzまで低下し、安定した回路動作が望めないことが判明した。

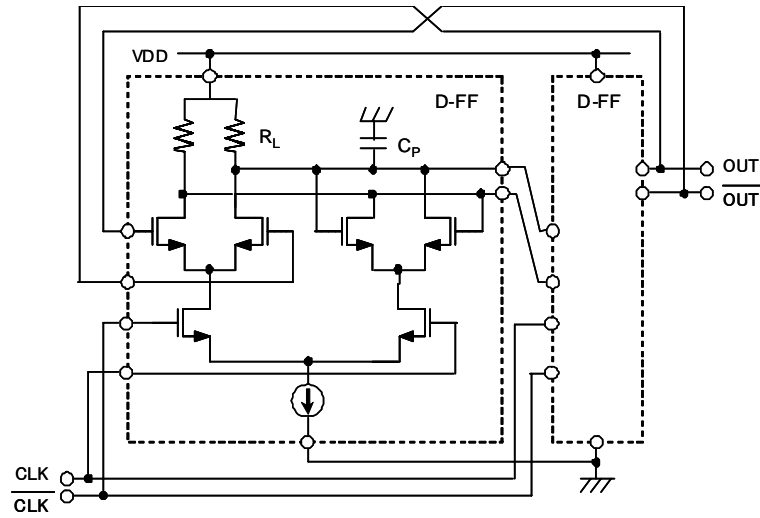


図 3.40 CML分周器回路図

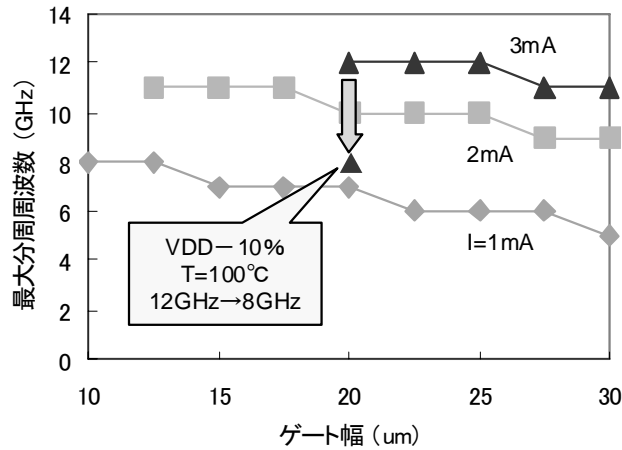


図 3.41 最大分周周波数

従来のCML分周器では負荷抵抗 $R_L$ と出力ノードの寄生容量 $C_P$ からなる時定数 $R_L C_P$ により性能が制限される。寄生容量はMOSトランジスタのゲート容量及びドレイン容量で決まるため、 $0.18\mu\text{m}$ 製造技術を使う限りは寄生容量の低減は望めない。そこで、この問題を回路的に回避するため、前項の差動回路と同様なオンチップインダクタを用いたピーキング技術の導入を検討した。インダクタピーキングを用いた分周器の回路図を図 3.42 に示す。負荷抵抗 $R_L$ に直列にインダクタ $L$ が接続され、 $L$ と負荷容量 $C_P$ の共振現象により回路の動作

速度を改善することができる。一般的に $L$ の最適値は、 $L_{opt} = \frac{R^2 C}{2}$  で与えられ、このとき回路の帯域は約 1.8 倍広帯域化できる。

図 3.43 に最大分周周波数の計算結果を示す。環境条件は、 $V_{DD}=1.8\text{V}$ 、 $T=25^\circ\text{C}$ である。MOS トランジスタのゲート幅  $W$  を 20、22.5、25  $\mu\text{m}$  とした場合について計算を行った。インダクタンスが 0 の点が従来の CML 回路の性能を示している。1.25nH のインダクタンスを使用し、 $W=20\mu\text{m}$  とすることで最大分周周波数を 38%改善でき、16.5GHz 動作が可能になる。また、 $V_{DD}$  を-10%、 $T=100^\circ\text{C}$ とした最悪環境条件下でも最大分周周波数の低下は 13.5 GHzにとどまり、安定な 10 GHz 動作が実現できる見通しが得られた。

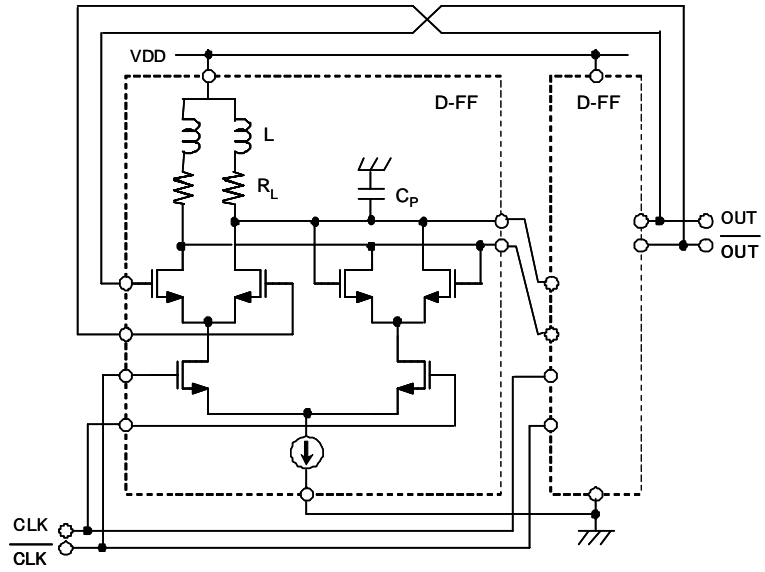


図 3.42 インダクタピーキング分周器回路図

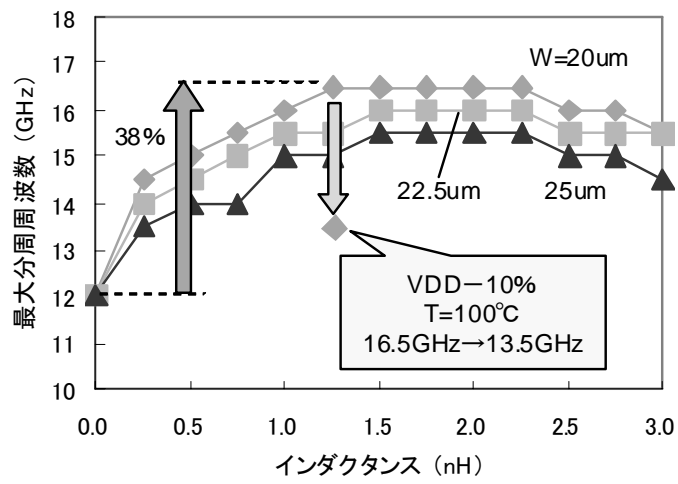


図 3.43 広帯域化後の最大分周周波数

しかしながら、1.25nHのオンチップインダクタの大きさは約  $270 \times 270 \mu\text{m}^2$ と大きいため、10 GHz分周器の大きさは図 3.44 に示すように  $570 \times 750 \mu\text{m}^2$ と非常に大きくなる。このことから、インダクタピーキングは安定な 10 GHz動作を保証するには必須の技術であるが、面積削減策を同時に検討する必要があることが明らかになった。そこで、10 GHz (10Gbit/s) 動作する回路ブロックを極力減らすハーフレート方式及びMUX/DEMUXの小型、低消費電力化の検討を行った。

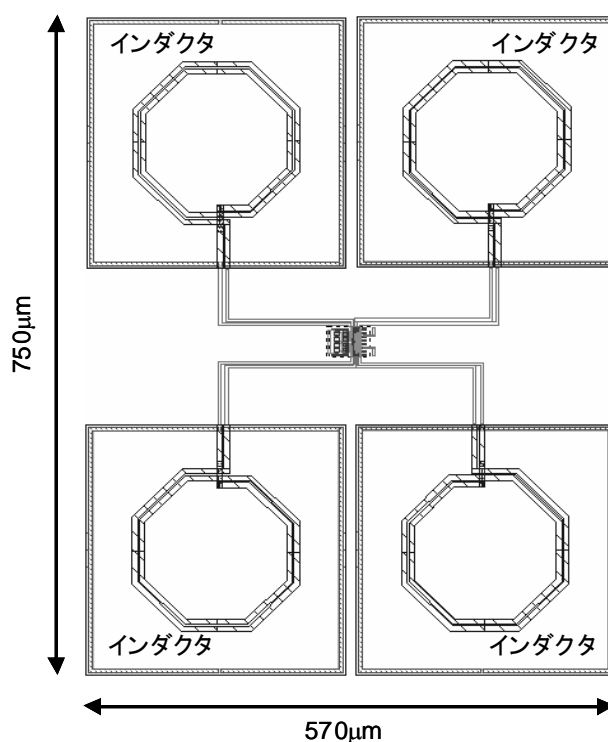


図 3.44 10 GHz分周器のレイアウト

### 3. 6. 4 ハーフレート方式

図 3.45 にMUX (クロック逡倍回路CMUを含む) で一般的に使用されるフルレート方式の回路構成を示す。ここでは 4:1 MUXの構成を示しており、2.5 Gbit/sの入力データ 4本を 10 Gbit/sのデータに多重する。4:1 MUXは 2:1 MUXをツリー状に接続し構成される。最終段MUXで多重化された 10 Gbit/sデータは、MS-FFで 10 GHzクロックによりリタイミング、

波形整形され出力される。MUXで使用する 5 GHz及び 2.5 GHzクロックはCMUと分周器 (Div.) により発生する。

この構成において、10 GHzクロック入力あるいは出力されるVCO (Voltage Controlled Oscillator)、分周器、クロックバッファ及びリタイミング用MS-FFが最も高速動作が要求される回路ブロックであり、これらの回路ブロックにはインダクタピーキングを用いる必要がある。回路ブロックの大きさを分周器を基準に見積もると、VCOが 1/2~1/4、クロックバッファは 1/2、リタイミング用MS-FFは 1 であり、これらの回路ブロックだけで分周器の 3 倍程度すなわち 1.3mm<sup>2</sup>もの面積を占有することになる。

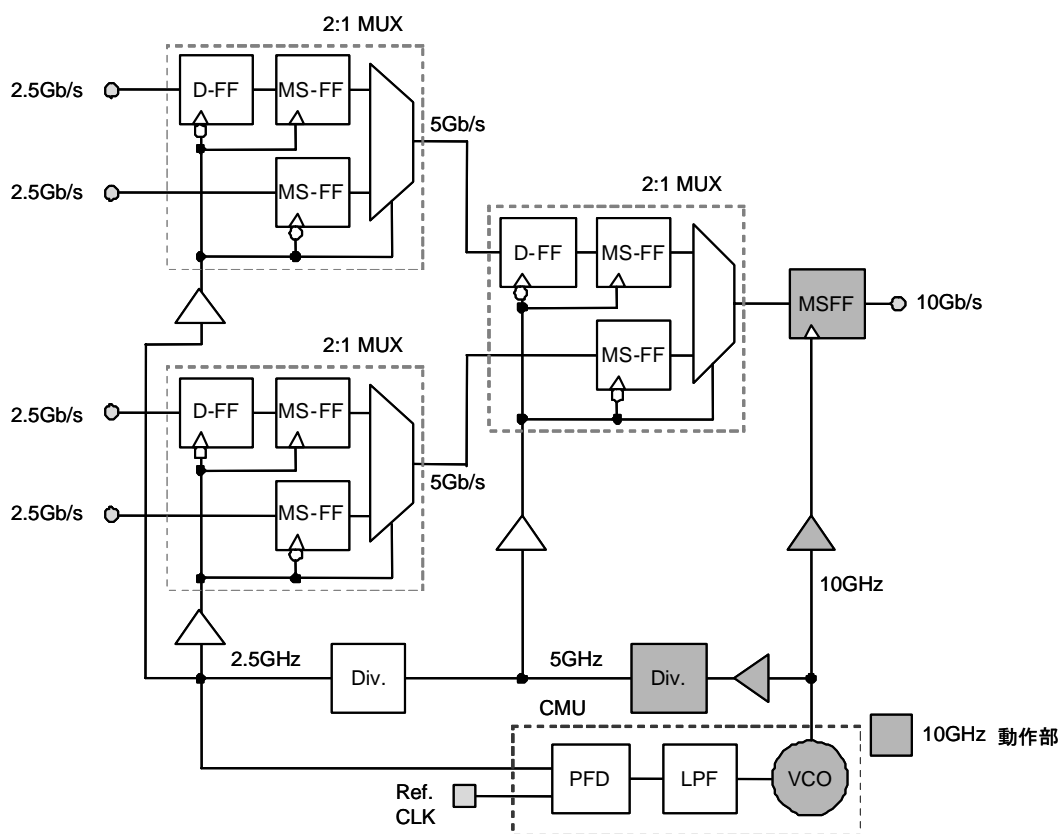


図 3.45 フルレート方式のMUX回路図

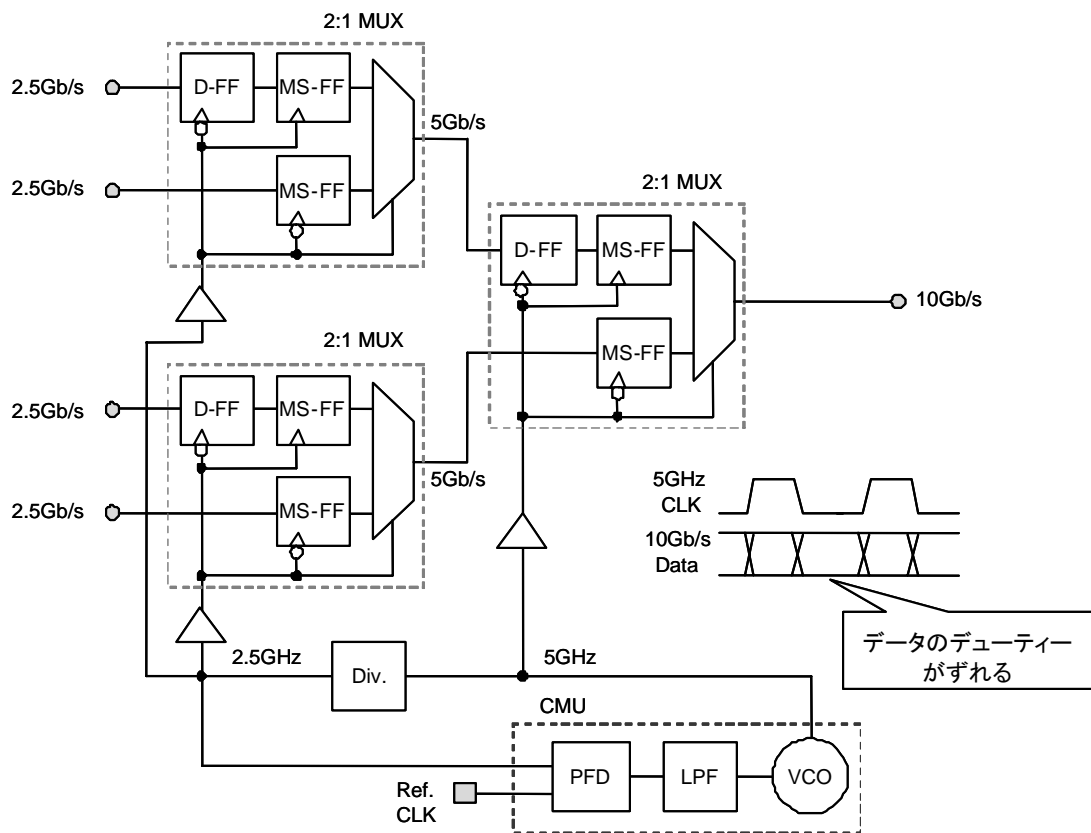


図 3.46 ハーフレート方式のMUX回路図

この問題を解決するため、ハーフレート方式の導入を検討した。ハーフレート方式では、図 3.46 に示すように最終段MUXで多重した 10 Gbit/sデータをリタイミングしないで出力する。これにより、10 GHzクロックが不要になるため、10 GHz動作する回路ブロックをなくすことができ、回路面積を大幅に削減できる。ただし、10 Gbit/sデータをリタイミングしないため、以下の 2 つの問題が懸念される。

- ① 5 GHzクロックのデューティがずれた場合、最終段MUXからの出力データ信号のデューティも同様にずれてしまう。
- ② リタイミングされないため、最終段 MUX で生じたパタンジッタはそのまま出力される。これらの問題を回避するには、



(1) クロック信号を差動信号にし、差動配線の長さや負荷容量を等しくする。

(2) 最終段 MUX のセレクタ回路の帯域を広くし、パタンジッタを抑える。

ことが重要である。(1)に関しては、クロック配線のレイアウトを対称化し、差動配線の負荷容量が等しくなるようにした。また、(2)に関しては、セレクタ回路にインダクタピーキングを導入し広帯域化を図った。

以上のように、ハーフレート方式を導入し、10 GHz 動作する回路ブロックをなくした上で、ハーフレート方式の欠点を補うため、セレクタ回路にインダクタピーキングを導入することで、電力及びチップ面積を大幅に削減することが可能になった。

### 3. 6. 5 小型、低消費電力 MUX 技術

上記の改良に加え、小型、低消費電力 MUX 技術を開発した。図 3.47 にハーフレート方式の MUX の回路構成を示す。2:1 MUX は、D-FF 1 個、MS-FF 2 個、セレクタ 1 個で構成されるが、D-FF 1 個、MS-FF 2 個はセレクタの入力（図中の A、B）におけるデータの位相を 90 度ずらし、セレクタの動作マージンを広げる役割を担っている。この構成において最終段 MUX に 5 GHz クロックを供給するクロックバッファ CKB の負荷は、D-FF 1 個、MS-FF 2 個、セレクタ 1 個であり非常に大きい。このため、CKB を通常の CML 回路で構成した場合、CML 回路の帯域は負荷抵抗  $RL$  と負荷容量  $CL$  の積で決まる時定数  $RLCL$  で支配されるため、5 GHz 動作をさせるには  $RL$  を非常に小さくする必要がある。これにより、CKB の消費電力は非常に大きなものとなる。これを避けるには、先に述べたインダクタピーキング技術を導入すればよいが、前述のようにオンチップインダクタの面積が大きいので、単にインダクタピーキングを導入することは望ましくない。

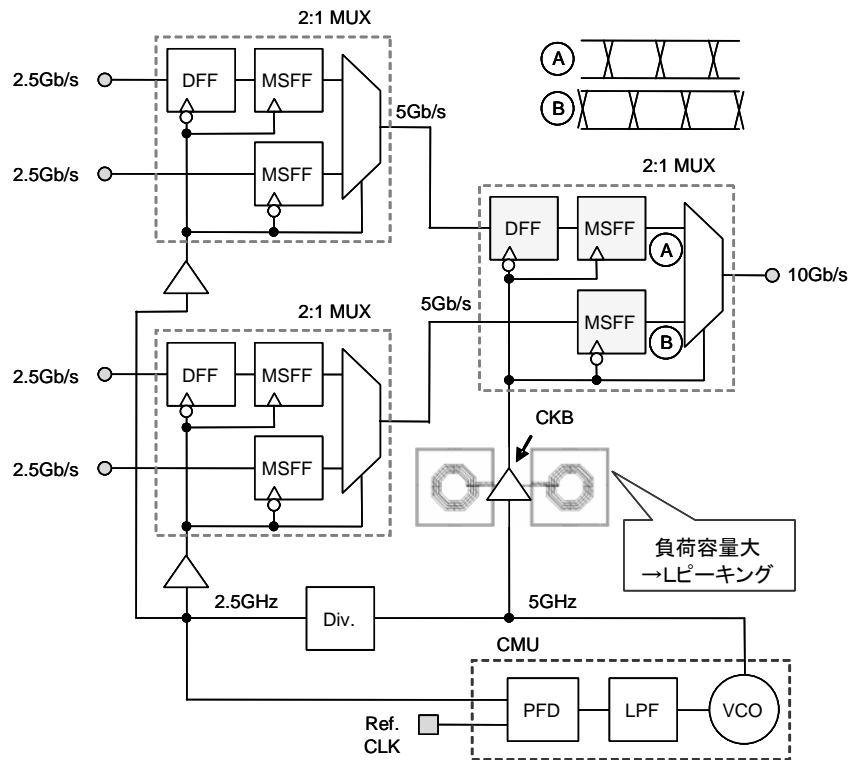


図 3.47 ハーフレート方式の MUX の従来回路構成

この問題を解決するために、図 3.48 に示す回路構成を提案した。この構成では、セレクタ入力 A, B におけるデータの位相をずらす D-FF 1 個、MS-FF 2 個を取り去り、その機能を低速側 MUX に供給する 2.5 GHz クロックの位相を一方だけ 90 度ずらすことによって代替している。これにより、5 GHz クロックバッファ CKB の負荷はセレクタ回路だけになり、従来に比べて大幅に負荷容量を低減できるので、インダクタピーキングが不要となる。また、5 GHz 動作の D-FF 1 個、MS-FF 2 個も不要となるので、消費電力も削減できる。

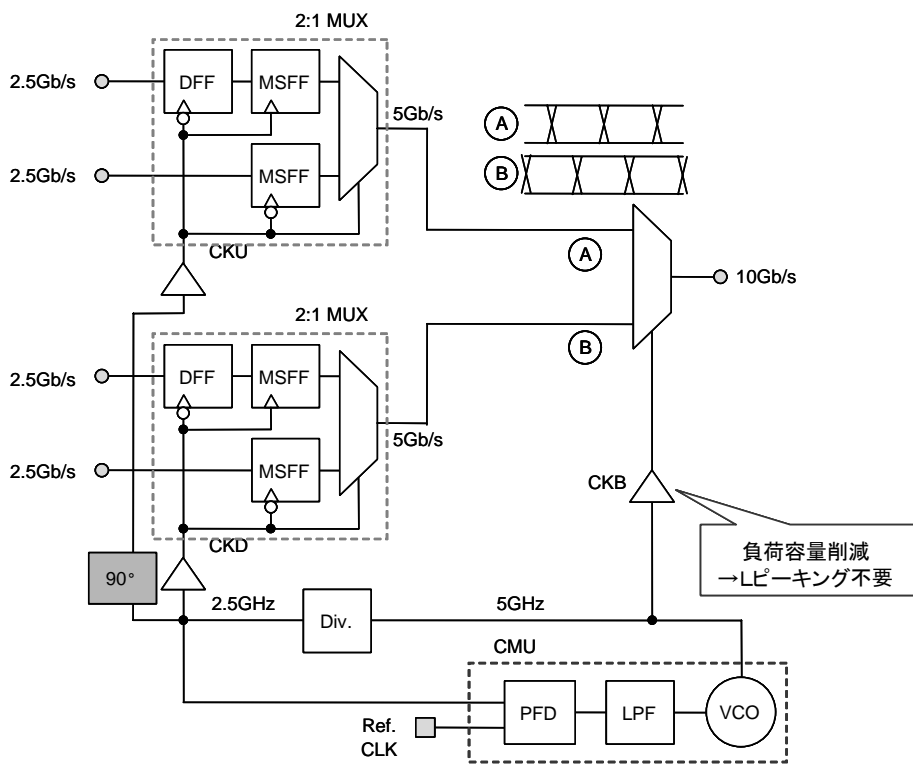


図 3.48 提案するハーフレート方式の MUX の回路構成

### 3. 7 LSI 化のための要素回路 TEG の試作、評価

以上述べた回路技術の有効性を実証するため  $0.18\mu\text{m}$  CMOS プロセスを用いて要素回路 TEG を試作、評価した。図 3.49 に試作したチップの写真を示す。試作チップは  $5\text{mm} \times 5\text{mm}$  で、9 個のサブチップからなり、4:1 MUX、1:4 DEMUX、EA-Driver、VCO が搭載されている。

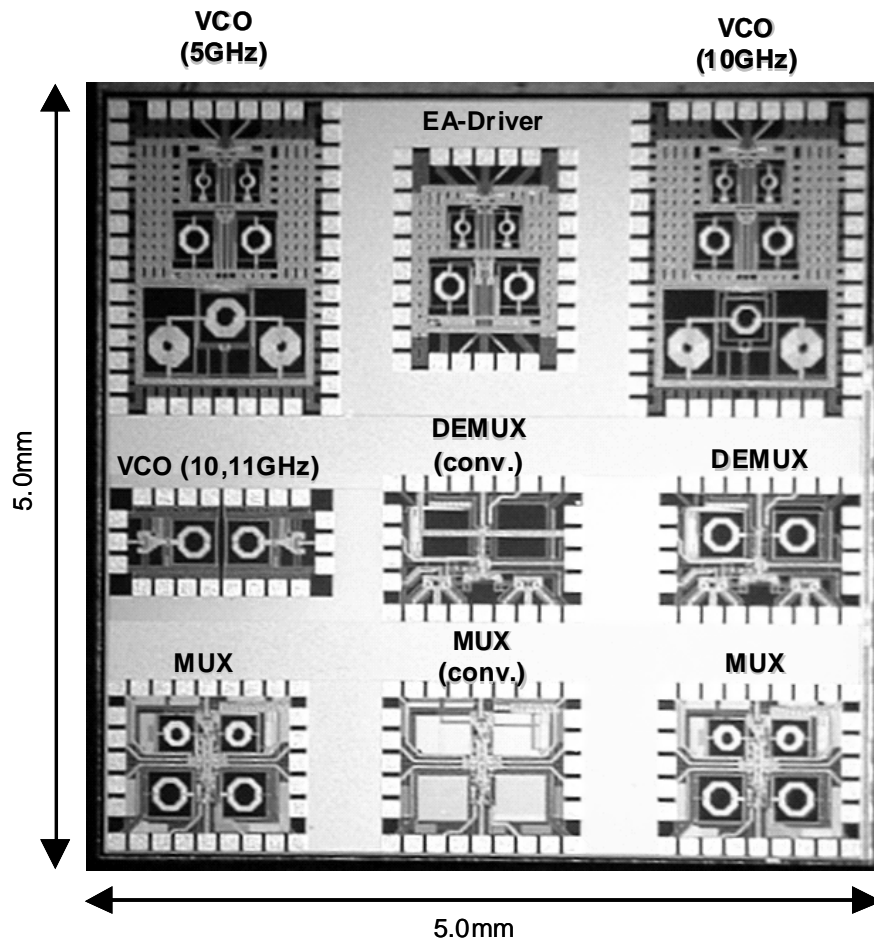


図 3.49 試作チップ外観

### 3. 7. 1 チップダイシングと評価基板実装

試作チップのダイシングと評価基板への実装は、(株)日本計器鹿児島製作所の協力の下に検討した。動作速度が 10 Gbit/s と高速なため、通常の市販パッケージに実装するとパッケージリードの寄生インダクタにより信号が大きく減衰するため、チップを評価基板に直接ボンディングする方法を採用した。

サブチップの大きさは 2mm 角以下であり、微小チップのダイシングに関しては新たな技術開発が必要となった。また、本要素回路 TEG はいずれも 10 Gbit/s という超高速で動作するためボンディングワイヤを極力短くする必要がありワイヤボンディングについても新たな最適化が必要となった。以下、チップ実装工程の概要とその最適化についてまとめる。

### 3. 7. 2 チップダイシング

図 3.49 のチップをそのまま評価基板に接着しボンディングすると、チップ中央部の回路ではボンディングワイヤの長さが 2mm を超え寄生インダクタンスにより回路本来の性能が評価できなくなる。そこで、チップダイシングを行い、各要素回路を分離した後に評価基板に実装することにした。チップダイシングは本来「ダイサー」という装置を用いるが、今回は、スクライブマシンを代用して分割を行うことにした。チップダイシングは図 3.50 に示すようにスクライブとブレイクという工程からなる。スクライブとは刃先の先端にダイヤモンドがついているダイヤモンドカッターを使い、これでチップ表面に V 字溝（スクライブライン）を刻む工程のことを指す。その後にブレイク工程を行う。この工程では、ウレタンゴムのテーブルの上に円柱状のローラーが横たわっていて、テーブルにチップを載せてテーブルを動かし、上からローラーの圧力でチップのスクライブラインに垂直な亀裂を入れ分割を行う。チップダイシングにおいてチップを欠けなくきれいに分割するために、カッター比重、カッター切り込み深さ及びローラー圧力の最適化が必要であった。以下に、これらの最適化のための検討結果をまとめる。

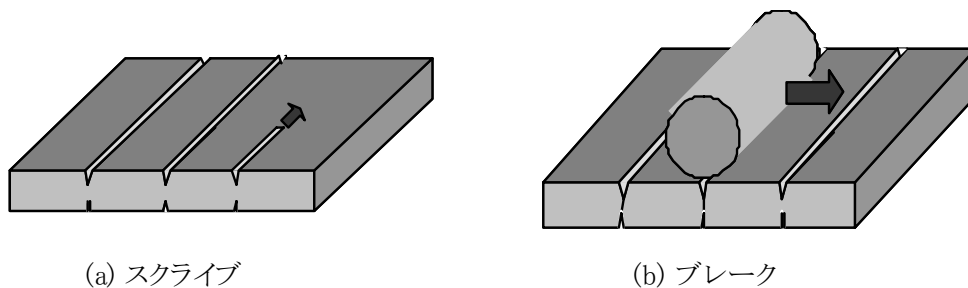


図 3.50 チップダイシング

(a) カッター荷重

チップに対するダイヤモンドカッターの荷重は、突然重くするとチップに余計な欠けが生じるため、0 g ~ 25 g まで 5 g 刻みで掛けることにした。またスクライブ回数は、各重さ 10 回とする。

(b) カッター切り込み深さ

チップに対してカッターの刃をどれくらいの深さで溝を彫るかを決める。今回は  $50 \mu\text{m}$  とした。

(c) ローラー圧力

チップに加わるローラーからの圧力は、上からの圧力が強すぎるとスクライブライン以外の所で割れ、多少の圧力でも垂直に割れず斜め方向に亀裂が入り、図 3.51 (a) のように他の要素回路部分を破壊することになる。今回試作した IC のチップの厚さは  $300 \mu\text{m}$  と厚いため、多少の圧力でもローラーからの圧力を受け斜めに割れてしまう。そこで装置目盛上  $0\text{kgf}/\text{cm}^2$  として、極力圧力が加わらない状態にして分割を行うことにした。その結果、図 3.51 (b) に示すように、きれいに分割を行うことが出来るようになった。

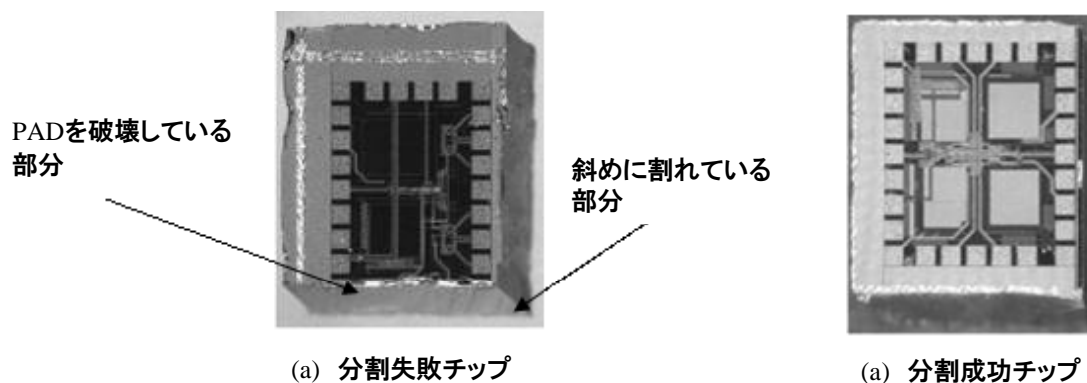


図 3.51 ダイシング例

### 3. 7. 3 ダイスボンディング

ダイスボンディングは、基板に銀ペーストを塗布し、その上にチップを乗せ高温でペーストを硬化させてチップを接着する工程である。今回の試作では、図 3.52 に示すように、ペーストの種類・硬化時間等は現場の設定をそのまま流用することにした。



図 3.52 ダイスボンディング

### 3. 7. 4 ワイヤボンディング

ワイヤボンディングとは、金線を超音波で接合部分にこすりつけて、チップ（または基板）との境目に化合物を成形して拡散接合させ配線を行う工程のことを指す。ボンディング形式にはボールボンドとウェッジボンドの 2 種類があるが、今回は、設備の都合上、ボールボンドの方式を取ることにした。図 3.53 にボールボンドのメカニズムを示す。

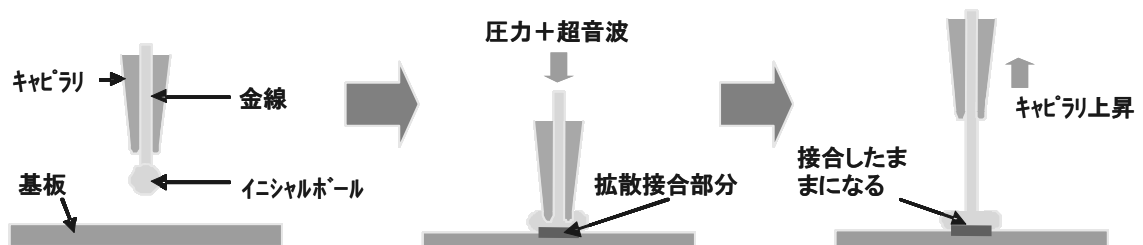


図 3.53 ボールボンディング

表 3.4 にワイヤボンディングの設定値を示す。今回の評価基板 (FR-4) に使われている材質 (ガラスエポキシ) は、超音波が逃げやすい特性を持っているので 2nd 側の US Time を長めに、US Power を強めに設定している。また、熱を加えると軟化するため、ヒータは入れずに常温でボンディングを行うことによってボンディング強度の確保をすることができた。

表 3.4 ボンディング条件

項目	1st	2nd	内容
US Power	5.2	7.0	超音波発振している振幅の量
Bond Force (g)	100	110	PAD面に接地したときに与える力
US Time (msec)	40	250	超音波を発振している時間
ヒータ温度	OFF (周囲気温 25°C)		ボンディング部分の温度

図 3.54 に実装基板の写真を示す。基板中央部にチップが配置されている (左の写真ではチップに保護キャップがかぶせてある)。チップは、右の写真のように実装基板に直接ボンディングされている。ボンディングワイヤの長さは約 1mm である。



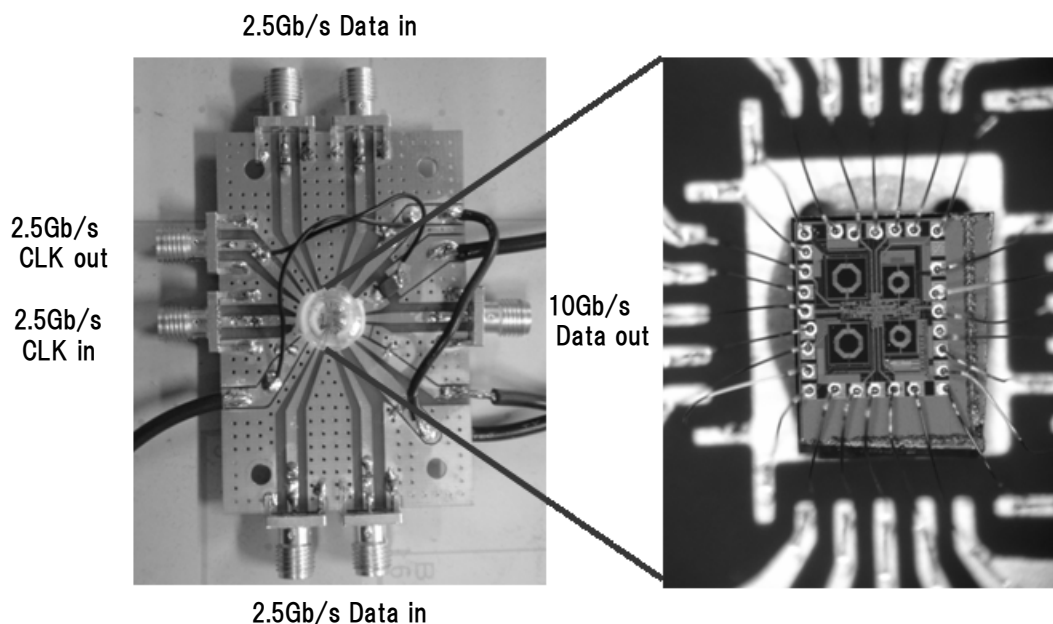


図 3.54 基板に実装されたチップ (MUX)

### 3. 7. 5 要素回路 TEG の評価結果

#### (1) EA-Driver

図 3.55 に EA-Driver の評価系を、図 3.56 に評価基板と EA-Driver チップのレイアウト図を示す。パルスパタンジェネレータで擬似ランダムパルスを入力し、サンプリングオシロスコープで出力アイパターンを観測した。シミュレーション及び測定したアイパターンを図 3.57 に示す。シミュレーション結果はレイアウトから抽出した寄生素子を用いている。実機結果はシミュレーションよりも  $T_r/T_f$  (立上り/立下り時間) が遅いが、十分なアイ開口が得られている。 $T_r/T_f$  が遅い原因は、IC のパッド容量やリードのインダクタといった外部的な要因が考えられる。シミュレーション波形の  $T_r/T_f$  に 2 重線が見られるが、実機波形にもその傾向が見られ、内部動作としては再現されていると考えられる。

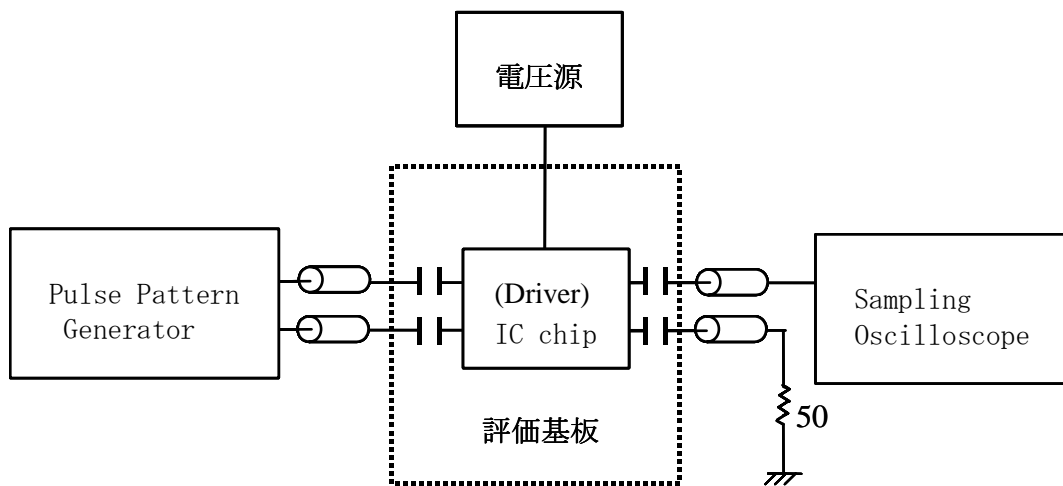


図 3.55 EA-Driver 評価系

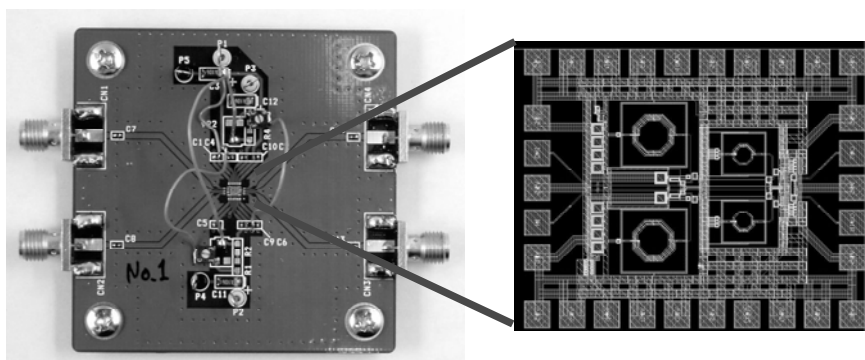


図 3.56 評価基板およびレイアウト図

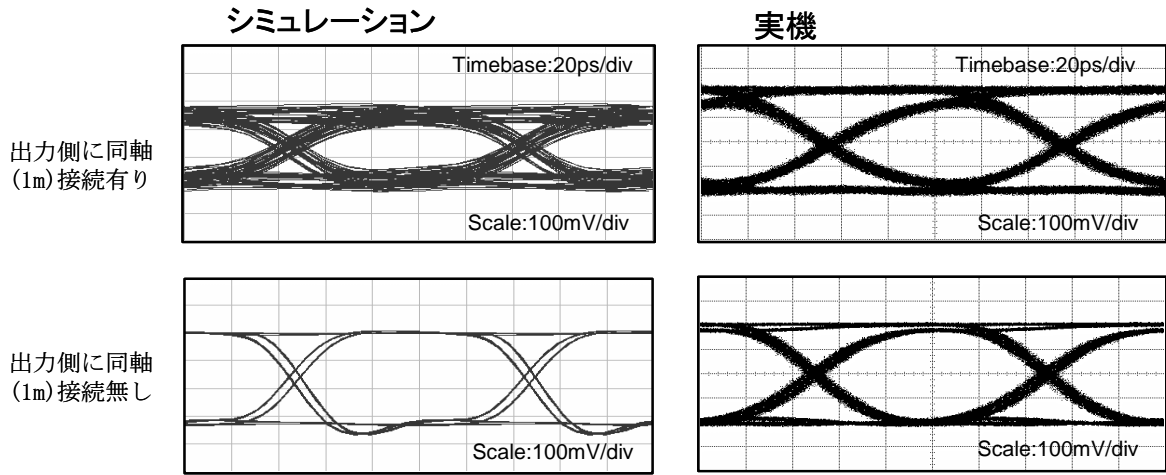


図 3.57 シミュレーション結果及び評価結果

今後の検討課題としては、 $T_r/T_f$ の改善、寄生容量の再見積り、ICの実装検討、配線容量やインダクタの影響を考慮した最適なレイアウト等の検討課題が抽出できた。

## (2) MUX

図 3.58 に 4:1 MUX の評価系と図 3.59 に 10 Gbit/s の多重動作波形を示す。パルスパターンジェネレータ (Pulse Pattern Generator) を用いて 2.5 Gbit/s のデータ信号を 4 本発生させ、4:1 MUX に入力している。多重された 10 Gbit/s 出力信号をサンプリングオシロスコープ (Sampling Oscilloscope) で観測した。4 本の入力端子のうち Din0 を” 0” に固定し、Din1 及び Din3 を” 1” に固定、Din2 に” 0”、” 1” の繰り返し信号を入力した。その結果、出力 (Dout) から期待通り” 01010111” のパターンが出力されることを確認した。この他にも数種類のデータパターンを入力し、いずれも正しい出力が得られることを確認した。10 Gbit/s 動作時の消費電力は 140 mW であった。

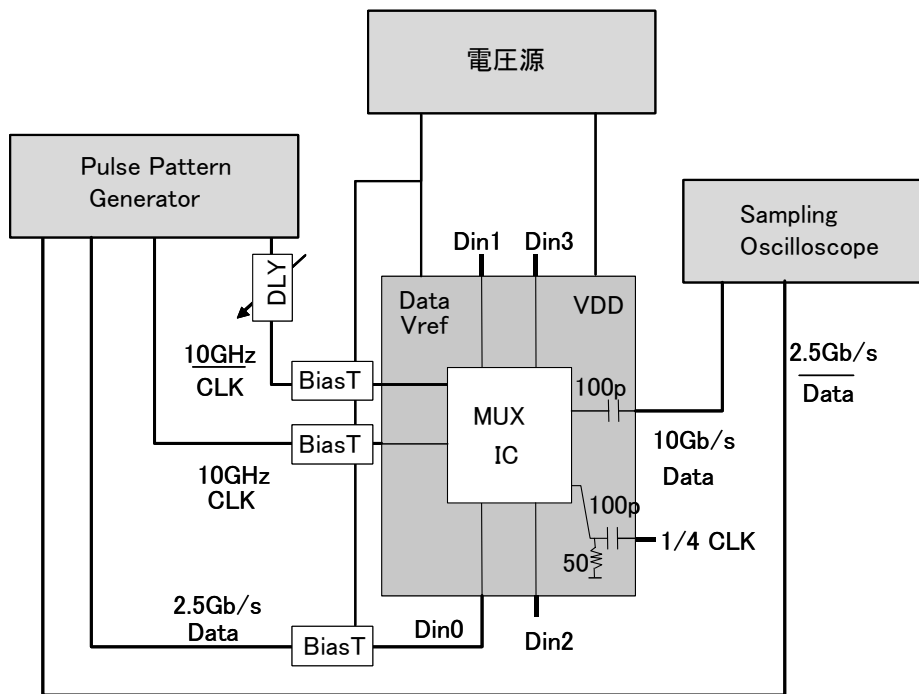


図 3.58 MUX の評価系

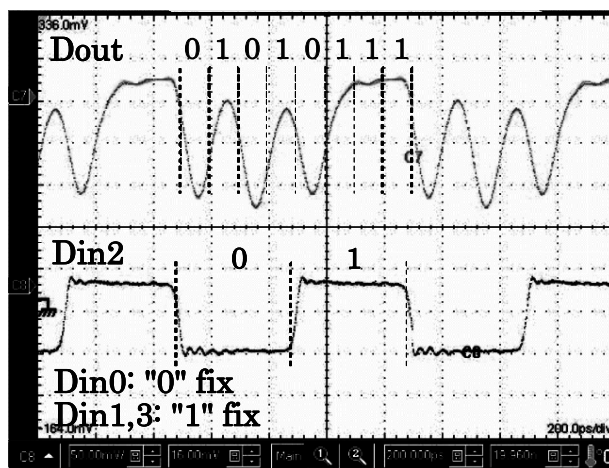


図 3.59 10 Gbit/s 動作波形

図 3.60 に 10 Gbit/s におけるアイパターンの設計波形と実測波形を示す。実測は設計に比べ  $T_r/T_f$  が大きく、ジッタも大きい大きなアイ開口が得られている。設計に比べ実測波形が劣化した原因は、①評価基板上のマイクロストリップラインでのロス、②出力信号の直流成分をカットするためにチップコンデンサによるロスと推定している。

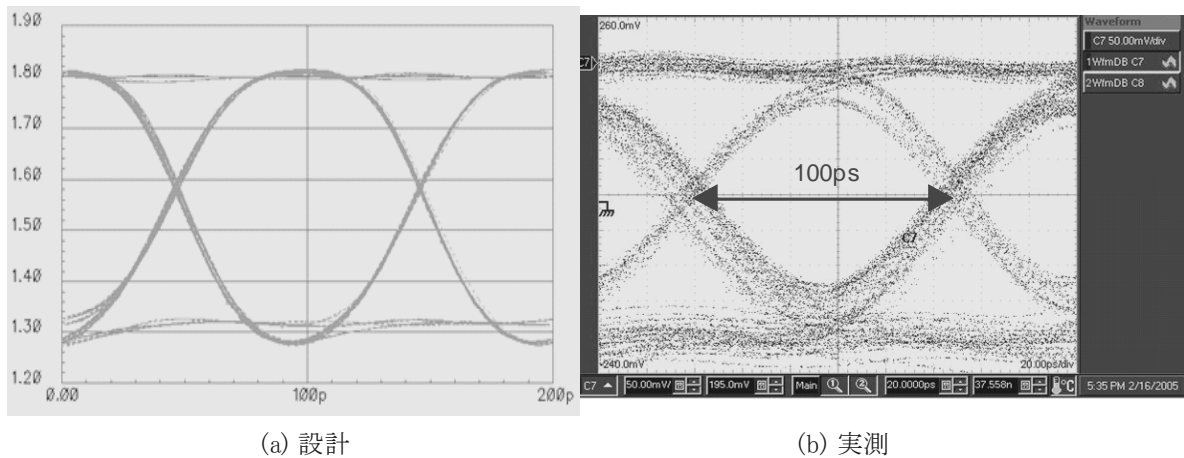


図 3.60 10 Gbit/s アイパターン

### (3) DEMUX

図 3.61 に 1:4 DEMUX の評価基板と、図 3.62 に評価系を示す。パルスパタンジェネレータ (Pulse Pattern Generator) で 10 Gbit/s のデータ信号を発生させ、1:4 DEMUX に入力し出力波形をサンプリングオシロスコープ (Sampling Oscilloscope) で観測した。

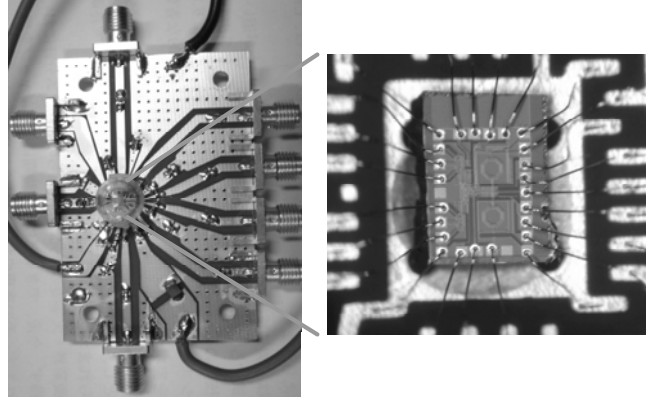


図 3.61 DEMUX の評価基板

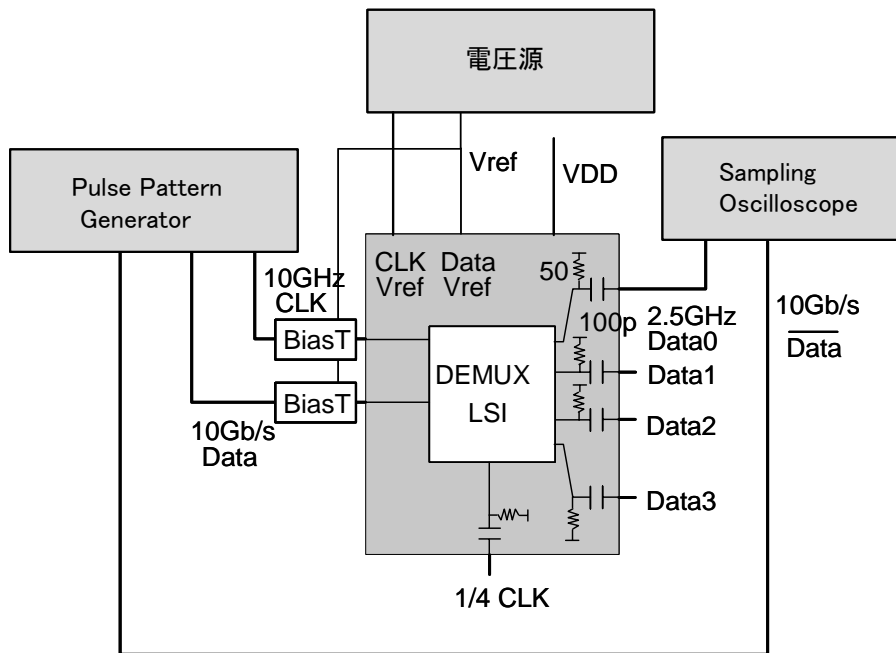


図 3.62 DMUX 評価系

図 3.63 に 10 Gbit/s における動作波形を示す。上段が入力信号の反転信号、下段が出力信号である。入力信号 Din が 4 ビットごとに出力信号 Dout0 に現れており、10 Gbit/s でデータ分離動作ができていることを確認できた。

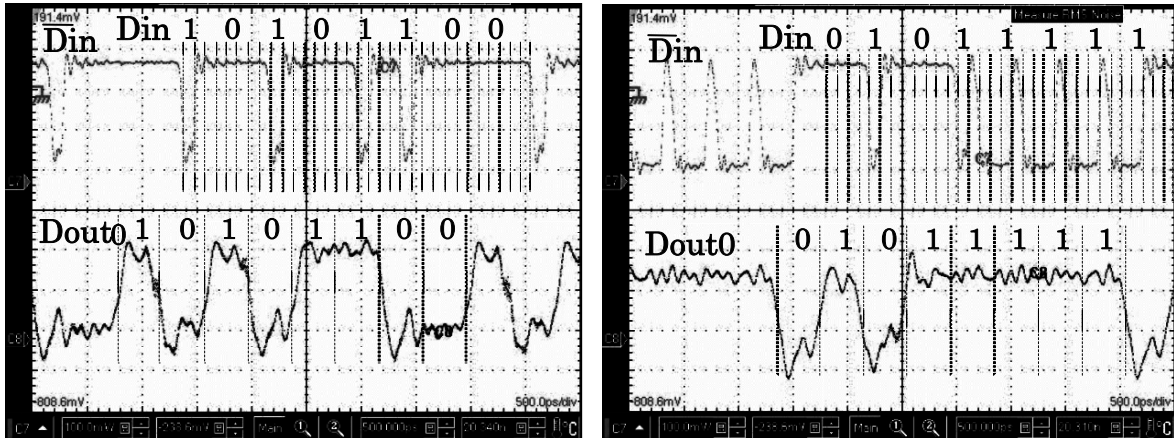


図 3.63 10 Gbit/s 動作波形

#### (4) VCO

図 3.64 に試作した VCO のチップ写真を示す。VCO は 2 種設計し、その中心周波数は 10 GHz と 11 GHz である。本 VCO はオンチップインダクタを 1 個しか使用しないので占有面積が小さい。また、負性抵抗回路を CMOS 構成とすることで発振振幅を大きくとり、等価的に位相雑音の影響を抑圧している。

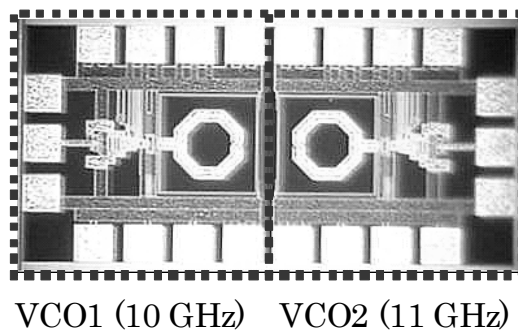


図 3.64 VCO のチップ写真

図 3.65 に周波数可変特性を示す。周波数可変範囲は VCO1（中心周波数：10 GHz）は 8.9～11.3 GHz、VCO2（中心周波数：11 GHz）は 10.2～12.3 GHz であり、いずれもほぼ設計どおりであった。図 3.66 と図 3.67 に位相雑音の測定結果を示す。離調周波数 1MHz、制御電圧  $V_{cont}=0V$  の時に、VCO1 は  $-102$  dBc/Hz、VCO2 は  $-105$  dBc/Hz であり、これらもほぼ設計どおりの結果が得られた。 $-100$  dBc/Hz 以下であれば 10 GHz CMU でも使用可能であることから、十分な性能を有しているといえる。また、出力回路を除く VCO のみの消費電力は 2.5 mW と小さい。

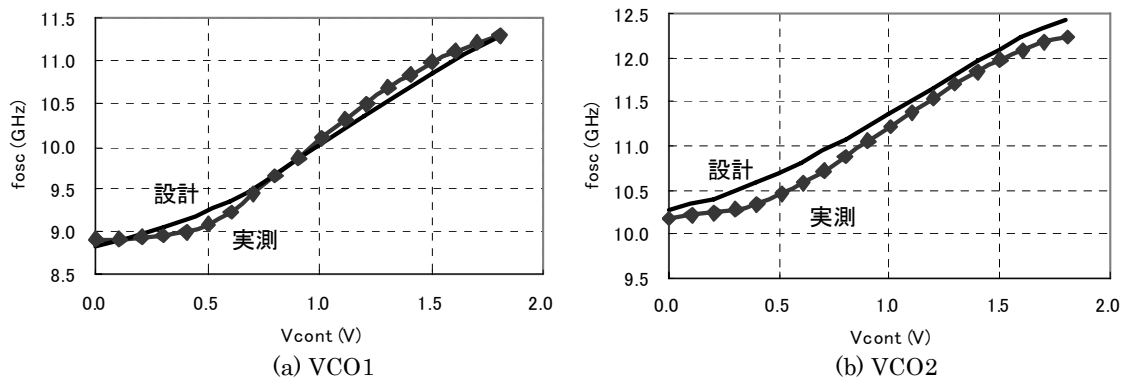


図 3.65 周波数可変特性

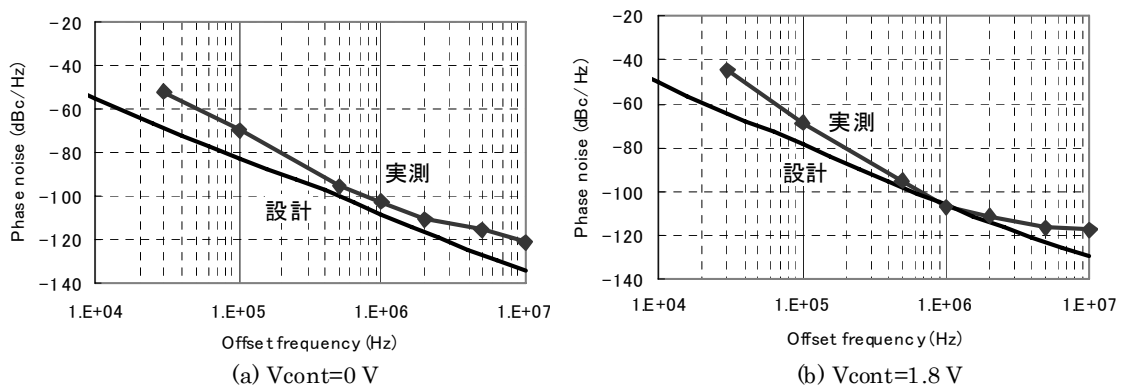


図 3.66 位相雑音 (VCO1)



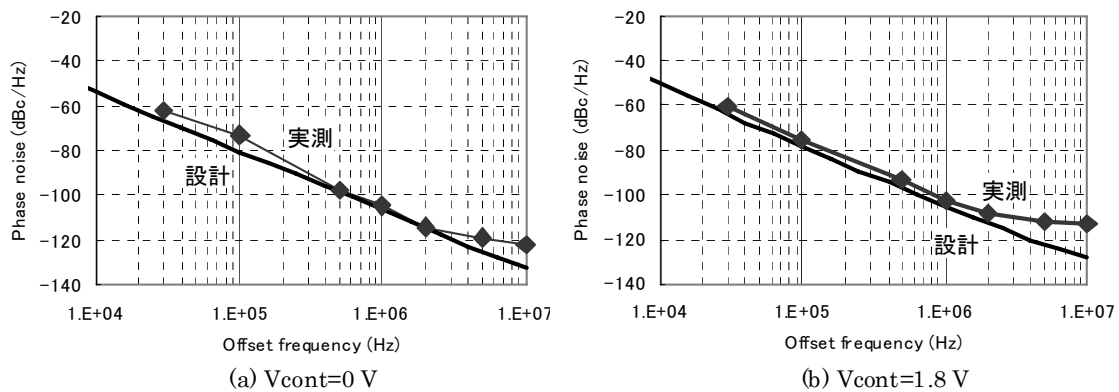


図 3.67 位相雑音 (VCO2)

以上述べたように、一部に課題は残したものの、要素回路 TEG の試作、評価により本研究で提案した回路技術の有効性を実証することができた。この結果を基に、これらの回路技術を総合し、インテリジェントアーキテクチャを具現化するシステム LSI の試作を行う。

### 3. 8 システム LSI の試作・評価

前項での要素回路 TEG 試作結果を基に、高速アナログ回路を搭載する主信号系と制御系をコントロールするデジタル回路、特に MPU コアも 1 チップの LSI に搭載した。LSI の試作においては、要素回路 TEG 試作の時と同様に考え、トランジスタは、CMOS の 0.18  $\mu\text{m}$  製造プロセスを採用することとした。特に今回は、提案するアーキテクチャを効率よく制御を行うために、専用の MPU を開発し採用することにした。

図 3.68 にシステム LSI のブロック図を示す。アナログ部とデジタル部のインタフェースをとる役割は ADC (Analog Digital Converter : A/D) および DAC (Digital Analog Converter : D/A) である。アナログ側からデジタル側へは、光送受信機のような特性をアナログ的に抽出した監視データを ADC でデジタル信号に変換し MPU へ送り制御のための

処理を行う。このデータの一部は、逐次メモリに蓄積しリアルタイムに状態を把握し、自律制御に役立てる。光送受信機の状態を最適にするための制御信号は、MPU で演算処理を行い、環境条件や光素子の経年劣化を考慮した最適化が行われる。この MPU で作られた制御信号（デジタル信号）は、DAC でアナログ信号に変換され、主信号系の各回路の制御を行う。

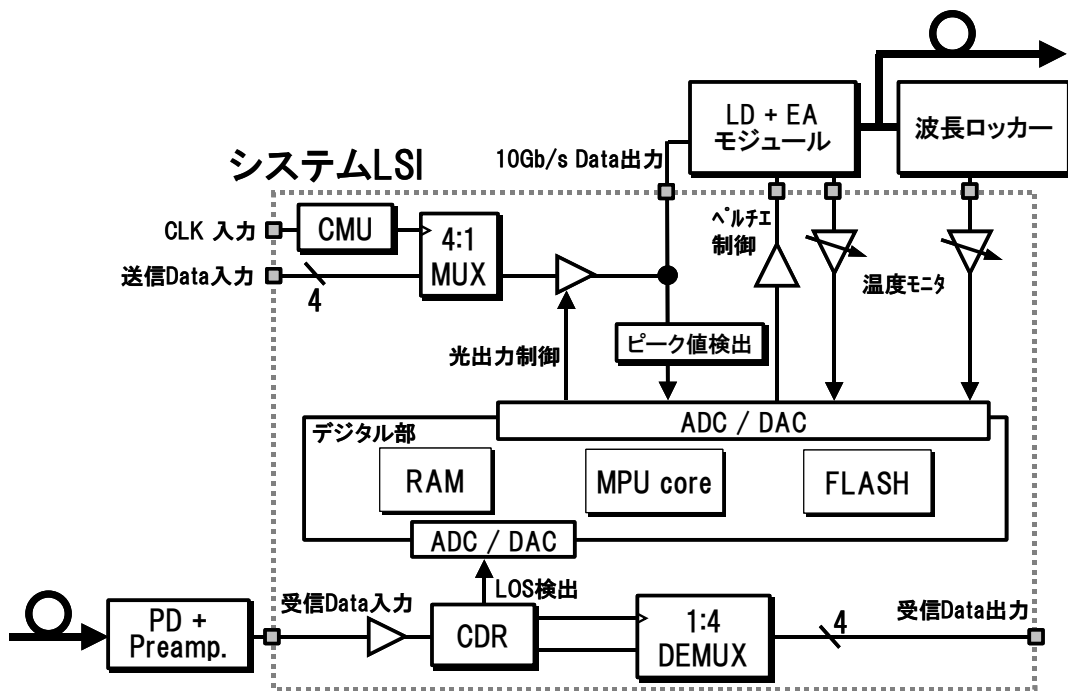


図 3.68 システム LSI のブロック図

### 3. 8. 1 MPU の開発

光送受信機を制御する MPU は、システム LSI として 1 チップに集積すること、今回適用する  $0.18\mu\text{mCMOS}$  プロセスで構成できること、また小型で効率の良い回路実装スペースを考慮し、本 LSI 専用の MPU を開発した。

まず、本 MPU で実行するアルゴリズムを検討した。アルゴリズムの構成を図 3.69 に示す。この図の 2 並列部、4 並列部は、それぞれ同じ計算 2 つまたは 4 つ並んでいる部分を指し、これらの演算アルゴリズムを高効率で実行することが望ましい。また、デジタルアナログ混在部、およびアナログ部設計側よりいくつかの要求事項があった。以上の要求事項

と解決法について述べる。

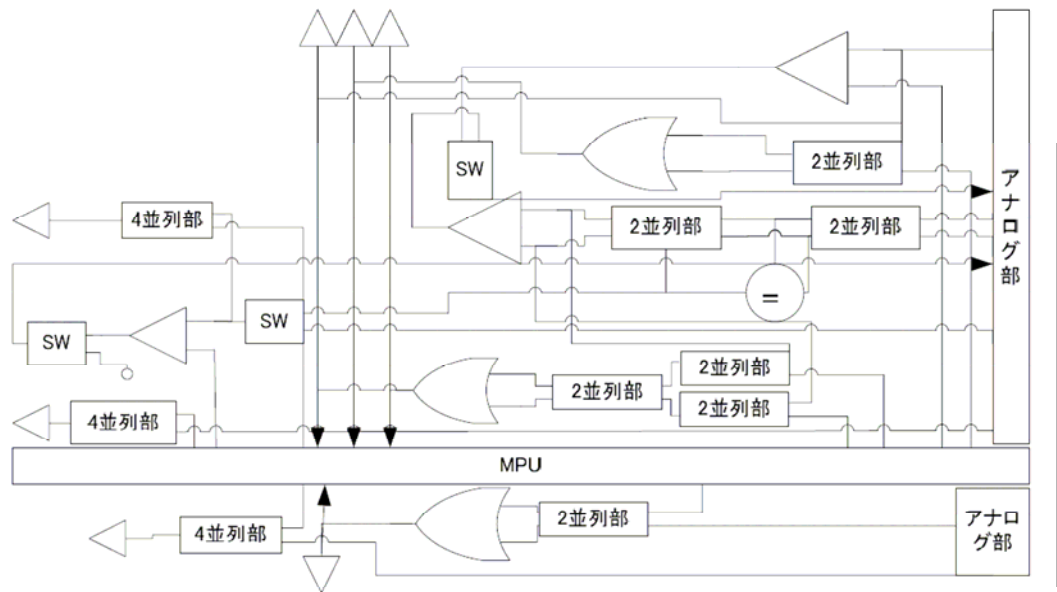


図 3.69 調整アルゴリズムの

(1) 処理の遅延時間

LD 発光レベルや波長測定など、サンプル時間や処理時間が厳密に定められているため、処理時間が完全に把握可能であり、かつその計測が容易であることが求められる。すなわち、決められた時間の計測や決められたインターバルでの作業、更には、命令サイクルから動作遅延の正確な計測が必要であった。そこで、クロックはデジタル/アナログ混在部と同一ソースのクロックで動作させ、全ての命令サイクルが 1 クロックで処理可能な構成とした。また、アルゴリズムの検討から用いるデバイスのテクノロジーから考えて実行時間は問題にはならないことが判明し、D/A 変換器やセンサそのものにある程度の遅延が存在するため、それ以上に高速化しても全体の高速化には直結しないと考えられる。従って、一般に用いられるパイプラインやマルチスレッド等の高速化技法は、本 MPU では用いていない。一方で、計測や制御のタイミングは一定とするためのタイマ機能を備え、ポーリングと割り込みによる一定時間間隔での時分割処理手段を提供している。また、メモリは、MPU の他にもデジタルアナログ混在部もアクセス可能であり、かつ同時に利用する必要がある

ため、デュアルポートメモリを用いた。この結果、MPU は、1 クロックサイクルで全ての処理を行う。更に同一クロック内にメモリの読み出しと書き込みを行うことも可能となった。但しメモリは同期式であるため、次のクロックでしか読み出し結果を利用できない。

## (2) 割込み処理

MPU コアは、I2C (Inter-Integrated Circuit) や RS232C のシリアルインタフェースを用いてオフチップ周辺機器との通信を行い、更に、これらの処理が通常処理に影響を及ぼすことが無いことが求められる。また、一定時間間隔で行わなければならない処理についてはタイマからの割り込みを利用する必要がある。そこで、それら全ての手段について割り込み処理を備えた。処理遅延を完全に把握するという要求から、割り込み発生した次のクロックで必ず割り込みごとに指定されたアドレスにサブルーチンコールを行う構造とした。全ての割り込みは他の割り込みとの重複が無ければ、必ず次のクロックで他の処理から移行し所望の処理が開始されることが保障される。また、割り込みはマスク機能と優先順位に基づく割り込み順序指定が可能であり、複数の割り込みが同時に発生した際には優先順位の高い割り込みから順に処理される。

## (3) 光 WDM 制御に特化した合理的なアーキテクチャ

本 MPU の主な処理内容は、複数あるパラメータを調整するためにその演算と I/O 書き込みを行うことである。これらの演算は基本的には同一演算処理の繰り返しにより調整を行い、入力と出力のセットで同時にセンシングと調整を行う。また、図 3.69 のように想定しているアルゴリズムにおいて 2 または 4 並列演算が多いことから、演算の並列度を 2 とするとアルゴリズムの効率の良い実行が期待できる。従って、演算処理を並列に行うことが出来れば処理能力が高められ、その並列度は 2 つあれば十分であると結論付けた。以上の見解から、MPU は、ALU を 2 系統備えることで 2 つの演算を並列実行可能な構成とし、専用の並列演算命令を備える方針を採択した。本命令セットを利用することにより低遅延で入力と出力の演算、もしくは 2 つの演算を同時に行うことができる。命令セットについても、柔軟なシフト命令とビット演算命令、1 クロックで動作する掛け算命令、スタック命令などが求められるため、これらの演算が並列で行える構成とした。ALU を 2 つ備えるため、条件分岐など一つ前の演算結果を利用する命令については、どちらの ALU の演算結果を利用するか指定が必要となる。そこで、より柔軟性を高めるため、それぞれの ALU について zero フラグ、carry フラグ、lower フラグを備え、両 ALU の AND/OR 条件を備えた。

#### (4) MPU の構成

デジタル部の全体のブロックを図 3.70 に、MPU 部のブロックを図 3.71 に示す。MPU 部のブロック図においては、デコーダからの信号線は省略してある。これは、デコーダがインストラクションメモリ以外の全てのモジュールに対して信号を送っているためである。デジタル部は I/O としては、前述のように RS232C シリアおよび I2C のインタフェースを備えており、割り込みによって MPU にアクセスを行う。具体的には、I2C からの EEPROM にあるプログラムの読み出し、シリアルからはデバッグや内部状態の通知、コマンドの読み取りなどが行われる。I2C では、通常通りクロックの立上りでサンプリングを行うのに対し、シリアルはクロックを持たないプロトコルであるため、ノイズに強くなるよう 1 ビットを 8 回サンプリングし、5 回以上検出できた値を読み取り値として用いる構造とした。MPU 部におけるデータの流れは次の通りである。レジスタ内部のプログラムカウンタに従ってインストラクションメモリを読み出し、デコーダに該当する命令を送る。デコーダがインストラクションメモリ以外の全モジュールへと適切な命令を送ることにより、各モジュールはそれぞれ適切な作業を行う。この MPU は ALU を 2 つ備えているため、レジスタの結果の受け入れ口も 2 つ持つ。また、メモリのリード・ライトの各セクタは 2 つの ALU と SP の 3 種類、データのセクタは、2 つの ALU からデータを選択する。プログラムの便宜を図るために専用アセンブラの記述も行った。専用アセンブラは通常の商用アセンブラが持つ基本機能を備えている。

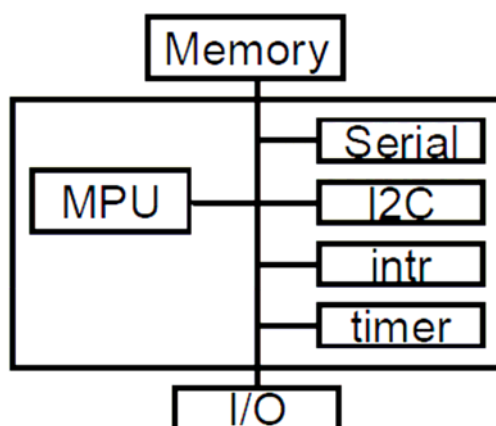


図 3.70 デジタル部の全体のブロック図

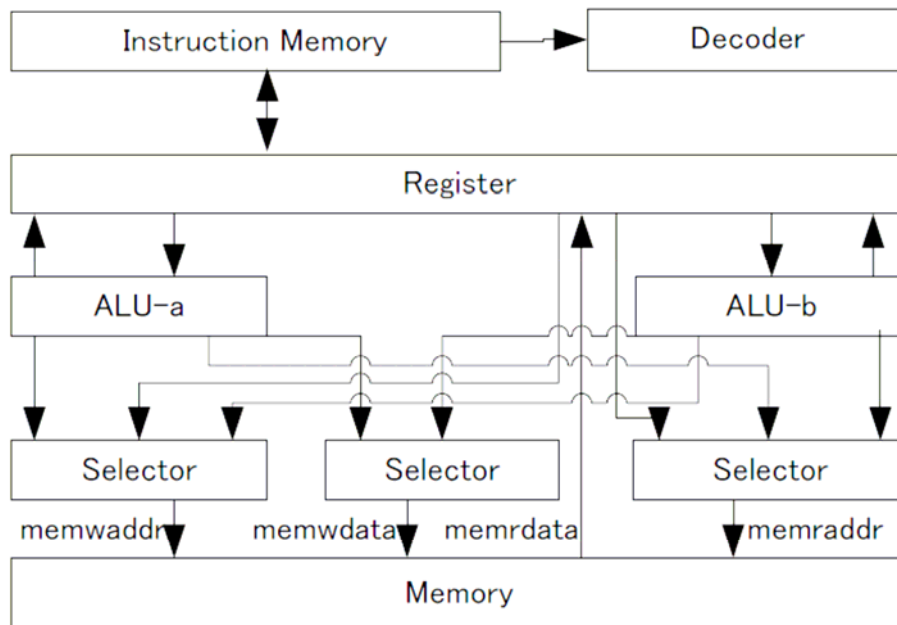


図 3.71 MPU 部のブロック図

### 3. 8. 2 試作・評価結果

図 3.72 に試作したシステム LSI のチップ外観を示す。チップサイズは、10mm×5mm 角であり、図の中央から左側がアナログ部、右側がデジタル部になる。アナログ部とデジタル部をそれぞれ単独で使えるように、間（配線途中）に I/O パッドを装備し、チップの中心で分割できるようにした。チップ内の実装は、それぞれの回路ブロックが動作時に発生するノイズの影響を極力抑圧するため、比較的小信号を扱い高感度な回路構成を多くとる受信 (RX) 部と、比較的大振幅の信号を扱う送信 (TX) 部との間にアナログインターフェースの回路を配置し、両者の配置間隔を大きくすることで送受信間のクロストークを抑えている。また、デジタル回路とアナログ回路の間も同様にスペースをとり、更に配線効率を考慮し ADC、DAC を配置している。同時に電源系統も分離することにより、デジタル回路からアナログ回路への信号ノイズの回り込みを防いでいる。

デジタル部は、配線効率を考え、中心に MPU コア部を配置し、メモリ (SRAM) で挟み込むようなレイアウトとした。

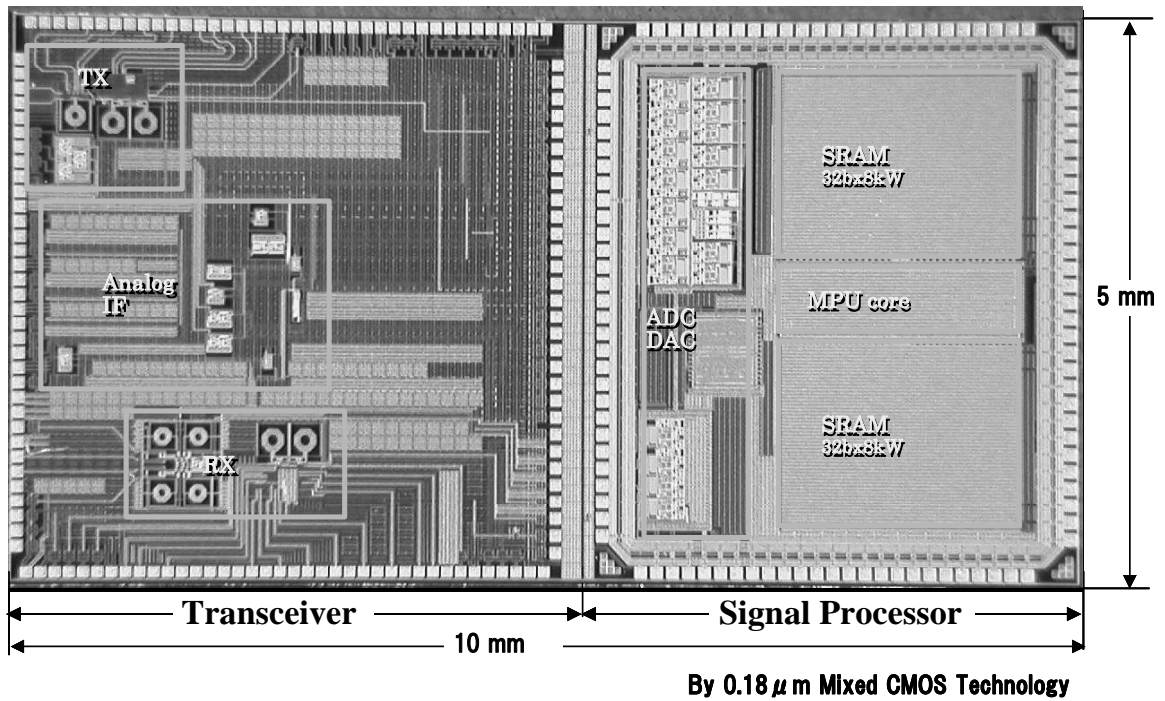


図 3.72 試作したシステム LSI のチップ外観

(1) 高速動作の確認

今回試作した LSI は、基本機能の確認が主目的であり、高速系の評価においては、信号の入出力部を中心にした MUX、DMUX で行った。図 3.73 に MUX、DMUX の評価系を示す。この MUX、DMUX の評価においては、10Gbit/s の信号入力に対しての対向試験とし、10Gbit/s 動作への適応性の確認を行った。

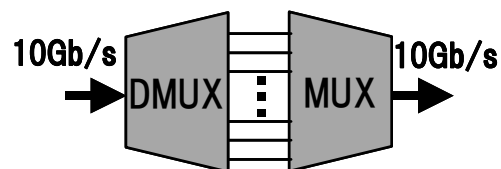
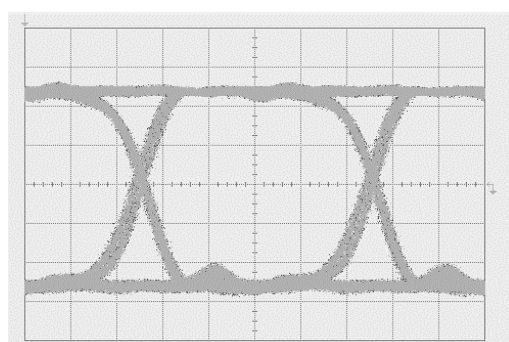
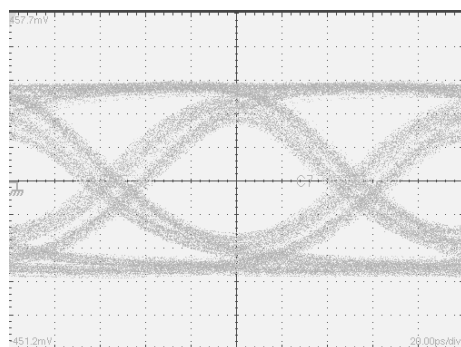


図 3.73 MUX、DMUX の評価系

図 3.74 に評価結果である 10Gbit/s の入出力の波形を示す。図 3.74 (a) は入力波形であり、図 3.74 (b) は、MUX の出力波形である。この波形からわかるように 10Gbit/s の伝送に対して十分な立上り/立下り時間を得られていない。これは、TEG 自作の時に比べ、統合的な LSI 化を行っているため、各回路ブロックに対して実装条件に制限があるため、主信号系の信号配線の長さが、最適化できていないための影響であると考えられる。



(a) DMUX 入力波形



(b) MUX 出力波形

図 3.74 高速動作の検証結果 (10Gbit/s  $2^{11}-1$  PRBS BER $<10^{-11}$ )

## (2) 制御系の評価結果

開発した専用 MPU を用いて光出力安定化のための APC と、LD の波長制御を行うために LD の温度制御を行うために重要な ATC の動作確認を行った。図 3.75 に APC 評価結果、図 3.76 に ATC 評価結果を示す。



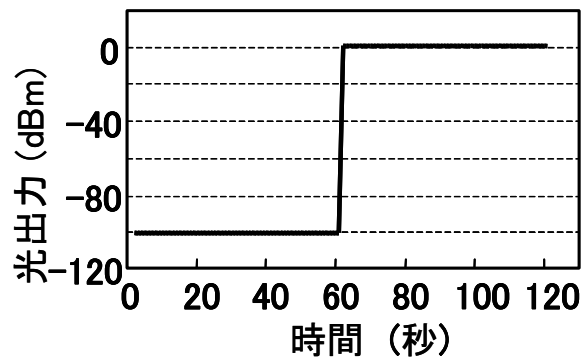


図 3.75 光出力の APC 特性

図 3.75 の APC による光パワー変化は、試験スタート後 60 秒後に光出力遮断（シャットダウン）信号を解除したと同時に、光パワーが 1.15dBm を中心に制御目標の $\pm 0.05$  dBm (1.10 ~1.20 dBm) 以内に瞬時に制御されている事が確認できた。

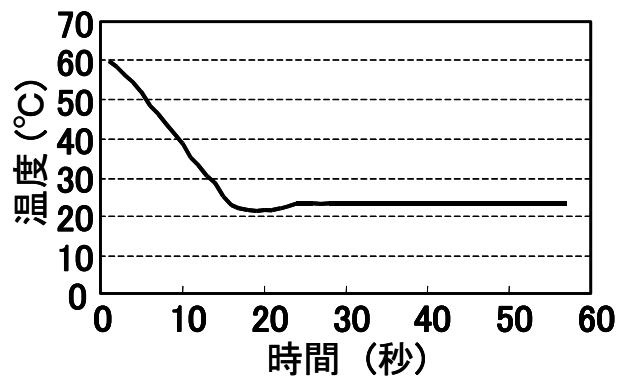


図 3.76 LD 温度の ATC 特性

ATC においては、図 3.76 より初期温度 60°C から 30 秒以内に一定温度 (23.1°C) 内に制御できている事が確認でき、ブレッドボードを用いたアーキテクチャの検証実験時 (360 秒) に比較すると、約 1/6 の時間に短縮することができた。

### 3. 9 まとめ

広範囲に亘る LD の製造バラツキや温度特性バラツキを吸収し、光送受信機自らの状態を常に自己学習、自律制御および自己診断する機能を具備するインテリジェントアーキテクチャを提案し、検証実験によりその実現性を明らかにした。検証実験では、シャットダウン解除後から、光出力電力モニタ較正、波長粗調整 (ATC)、光出力電力調整、波長微調整 (AFC) と、順次、自動制御を行ったが、何れも正常に動作していることを確認できた。また、波長や光出力電力が定常状態に収束するまでの所要時間を 360 秒に抑えることができ、調整時間の大幅な短縮が可能であることを確認できた。更に、光送信波形情報を送信機にフィードバックし、光送信アイパターンのクロスポイントや消光比の最適化を自律的に行う手法の有効性も検証できた。

また、主信号系のアナログ部と、独自に開発した MPU を搭載するデジタル部を混載させ、基本動作確認のためのシステム LSI を試作し、制御時間を 1/6 に短縮することができ、更に 10Gbit/s の高速動作を確認することができた。まだ、安定した 10Gbit/s 動作を継続するには課題が多いが、それぞれの課題の抽出を行い、次章で述べる光通信量子暗号伝送装置に積極的に適用できるよう改良を加えていく予定である。

## 第4章 光通信量子暗号伝送装置の開発

### 4.1 緒言

近年、インターネットを中心にネットワークを活用したネットバンキング、ネット決済、ネット取引等のビジネスが急速に普及し始めており、金融情報や個人情報をはじめとする機密情報伝達にも利用されるようになってきた。このため、ネットワークの安全性が強く意識されるようになり、図 4.1 のような従来の数理的な安全性から図 4.2 のような物理的に安全性を保證できるネットワークの開発が急務になってきている。現在のネットワークにおける情報の安全性保護には様々な数理的計算処理を用いた暗号が利用されてきている。しかし、これら数理暗号は定量的な安全性の証明はされておらず、将来コンピュータの処理能力の向上や暗号解読アルゴリズムの発見により安全性の低下は避けられない。また、完全な安全性を保障できると言われている暗号方式の **One Time Pad** では、鍵配送の安全性がボトルネックとなり実現が困難であった。この問題を解決するため、量子力学的な効果を利用し、単一光子伝送を採用した **BB84** などの量子鍵配送方式がある。この方式は量子デバイスの発展により格段の進歩を遂げているが、原則として単一光子の伝送を行うため、通信速度の高速化は原理的に困難であり[13]、**One time pad** と組み合わせる究極の暗号として、現在のブロードバンドネットワークに適用することは難しい。したがって、種々の暗号システムのための鍵配送としての応用が期待される。一方、2000年に **Yuen** によって開発された **Yuen-2000** プロトコル (**Y-00**) は光信号の観測時に発生する量子揺らぎ（量子雑音）によって、盗聴者の取得データを暗号化する方式である[14]。これは従来のストリーム暗号の機能を量子雑音によって実現する方式であり、暗号化速度、データ通信速度に原理的な限界がないという特徴を持つ。また、安全性は基本 **Y-00** に対する種々のランダム化法と盗聴者の量子力学的検出能力に依存するが、基本的な **Y-00** であっても安全性が定量的に保證可能な暗号となる[15][16]。

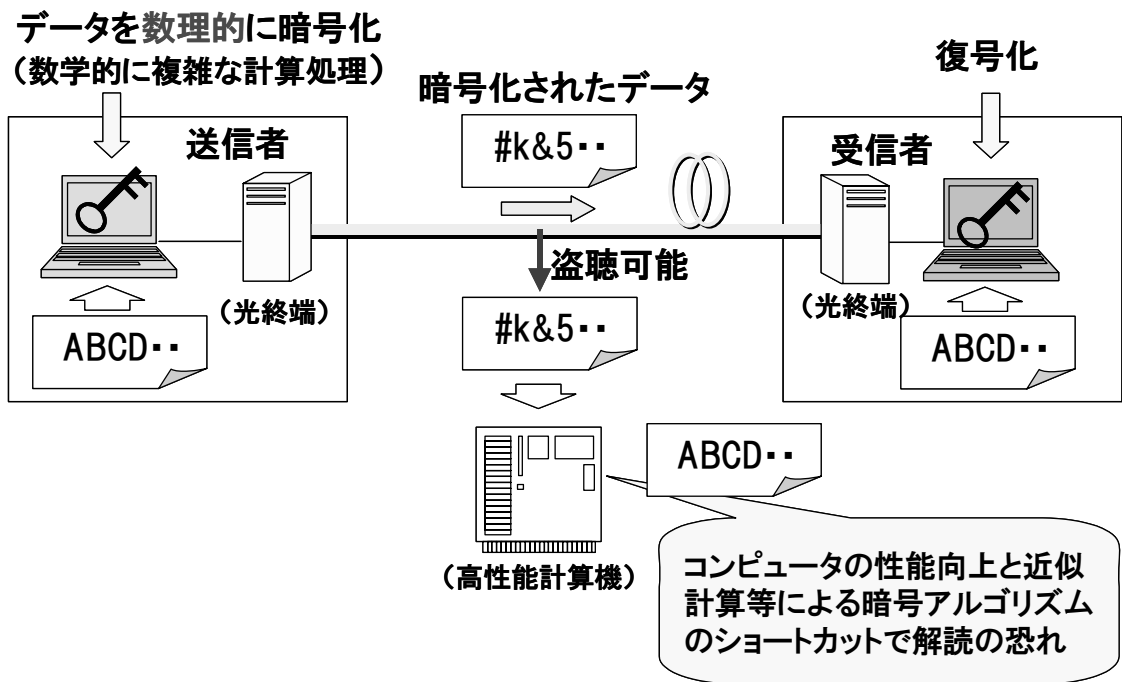


図 4.1 現在の暗号伝送

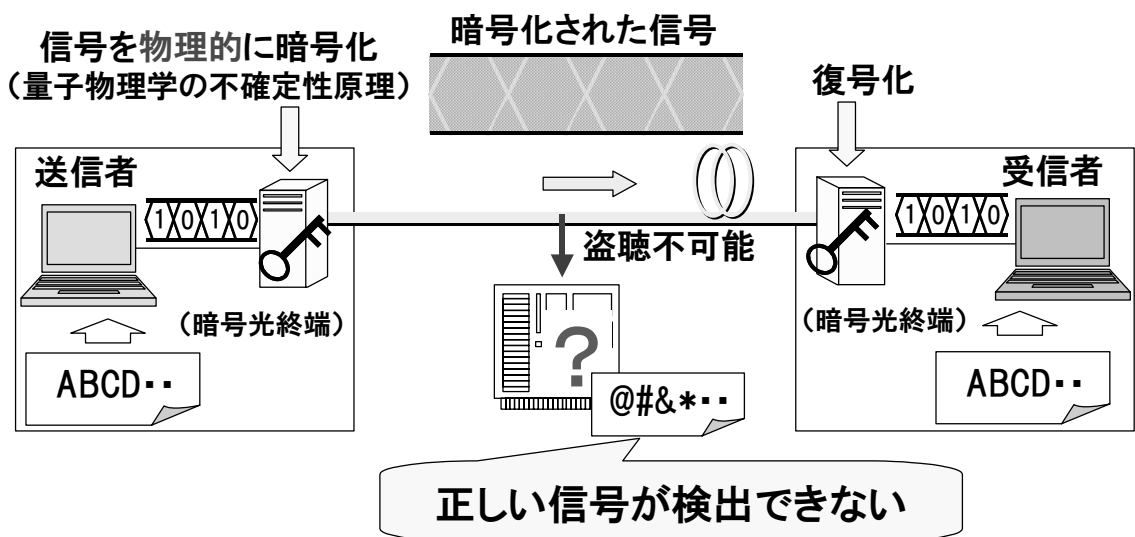


図 4.2 量子暗号伝送

本研究では現在のブロードバンドネットワークに適用可能な量子現象を応用した高い安全性を保証できる暗号通信の実用化を目指し、強度変調方式による[17][18] Y-00 光伝送装置の開発を進めている。

Y-00 の基本モデルは、共通鍵による優位性を用いて盗聴者の S/N (あるいは誤り率特性) を劣化させることによる暗号構成の原理 (優位性創成原理) を示すものであり、それだけで究極の安全性を実現するものではない。しかし、それでも既存の攻撃理論に対して鍵長の指数関数的安全性が達成できる[27]。実際アメリカでの実験の鍵長は 4000 ビットである。一方で Gbit/s 級の超高速化を目指すために鍵長を短くする必要がある場合や完全性を目指すときには、基本モデルに種々のランダム化を採用することによって安全性の強化や計算量的に完全な安全性が実現できることが示されている[27]。本論文では Y-00 方式を実装するための基本回路の実現方法、更に短い鍵長モデルの安全性を改良するために提案されている種々のランダム化手法を実装するための回路構成法を検討し、実装実験を進めてきている。現在、この方式の送受信機を製作し、商用回線を用いた 2.5Gbps、192km 多段中継伝送を実施し、量子暗号通信の新たな展開を示してきた[19][20][21][22][34]。

本方式はデータ伝送に光強度変調方式を用いているため、既存の公衆通信ネットワークとの親和性が高く、商用基幹ネットワークをはじめアクセスネットワーク等への適応性が非常に高いのが特長である。また、動作環境等の特殊な制限も無く LSI 化が容易なため、既存の光伝送装置等への組込みが可能なことも強みである。

本章では、4. 2 項で Y-00 方式の暗号化原理について概説する。次に、4. 3 項では、試作した光送受信機の構成を、4. 4 項では、Y-00 方式光送受信機の試作結果について述べる。4. 5 項では、更に改良を加えた Y-00 トランシーバの開発について述べる。4. 6 項では、稼働中の商用回線を用いた Y-00 方式の現場実証試験の結果について述べ、高速・大容量伝送が可能であり、既存通信プロトコルへの適用および安全性との両立ができることを示す。4. 7 項では、10Gbit/s 伝送への適応性の検討するため 10Gbit/s 伝送装置の開発について述べ、4. 8 項で本章全体の結果を要約する。

#### 4. 2 光通信量子暗号 (Y-00) 方式の暗号化原理

一般に、光信号を観測する際に発生する量子雑音による通信の限界は、厳密な量子信号検出理論によって評価可能である[23][24][25]。Y-00 方式は、図 4.3 で示すようにコヒーレ

ント光源として用いるLD光を強度変調し、その光信号を観測したときに不可避に発生する量子雑音を利用して物理的に正規受信者と盗聴者の受信感度に差をもたせ、データを暗号化する方式である。その量子雑音の効果は、上記の量子信号検出理論によって厳密に評価されるので、暗号としての能力が定量化可能と期待されている [26]。

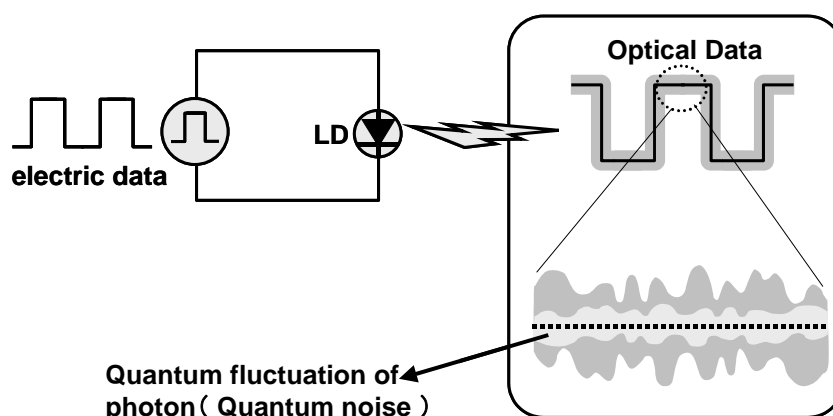


図 4.3 光強度変調における量子揺らぎの効果

#### 4. 2. 1 暗号化原理

光強度変調を用いた Y-00 方式では、暗号化のため多値の光強度レベルを用い、このレベルの中から 2 値のデジタル情報を選択して伝送を行う。Y-00 方式の基本的なコンセプトは、変調をかけた LD 光を観測したときに発生する量子揺らぎ（量子雑音）を暗号化に利用することにある。即ち主信号は、量子雑音が多値信号レベルの識別判定に影響を及ぼす領域まで隣接信号レベルを接近させ、盗聴者が信号レベルを観測するときに量子雑音によって生じる S/N（信号電力対雑音電力比）劣化の効果で主信号レベル検出を不可能にする。送信者は多値化された主信号を 1 ビット毎に 2 値レベルの組合せ（基底）に振り分け伝送を行う。暗号の復号は、送受信間で共通鍵を利用し、基底情報を共有し合うことで基底情報に合わせた信号識別の閾値をビット毎に移動させ信号の復号を行う。この方式は主信号そのものに暗号処理をリアルタイムに、且つ高速に施すことができるため、高速・大容量伝送

への適用に期待できる[28][29]。

通常の光伝送波形を図 4.4 (a) に示す。信号は光のパワーレベル差を用いて、“0”、“1”の2値の光強度変調されている。この2値の信号の観測時（光/電気変換時）に発生する量子雑音は、図 4.4 (b) のような分布になっており、その発生確率は周知の通りポアソン分布となる。ここで光パワーが大きい場合、ガウス分布に近似することができる。また、本論文では量子雑音効果を正しく考察するため、送受信機で発生する熱雑音等の古典雑音は0と考える。この2値の強度変調の場合“0”、“1”の消光比を十分確保することにより、上記雑音の影響を受けないところで受信信号の“0”、“1”の識別を行う。

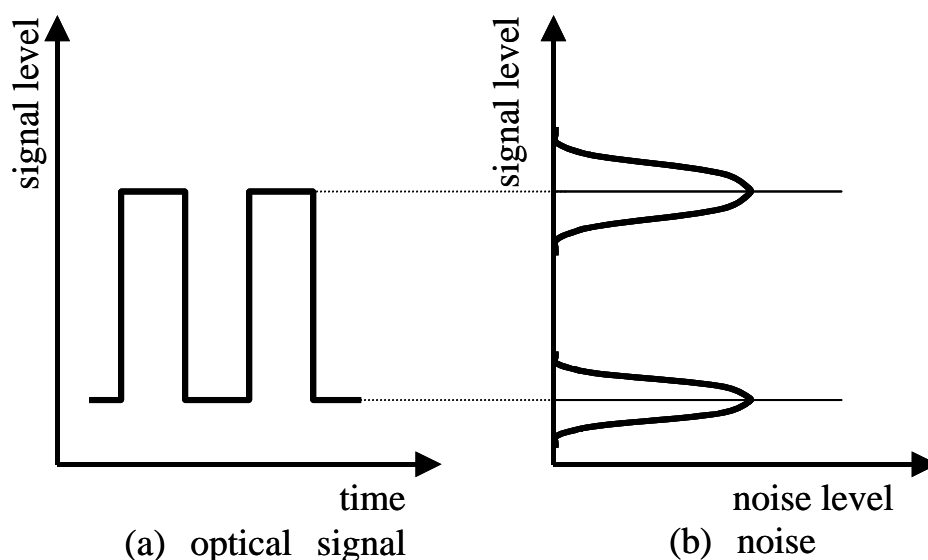


図 4.4 光信号とノイズ

極端に消光比を小さくすると図 4.5 (a)、(b) のような関係になり、雑音の分布は重なり合う部分が発生し受信時の信号識別に影響を及ぼすため、ビットエラーレートは悪化し受信感度が劣化する。この光信号の観測時に発生する量子雑音は、重ね合わせの量子状態を観測することにより量子の重ね合わせ状態が崩される際に起こる量子揺らぎ現象である。この雑音の発生は完全にランダムであり、人為的に除去することは不可能である。

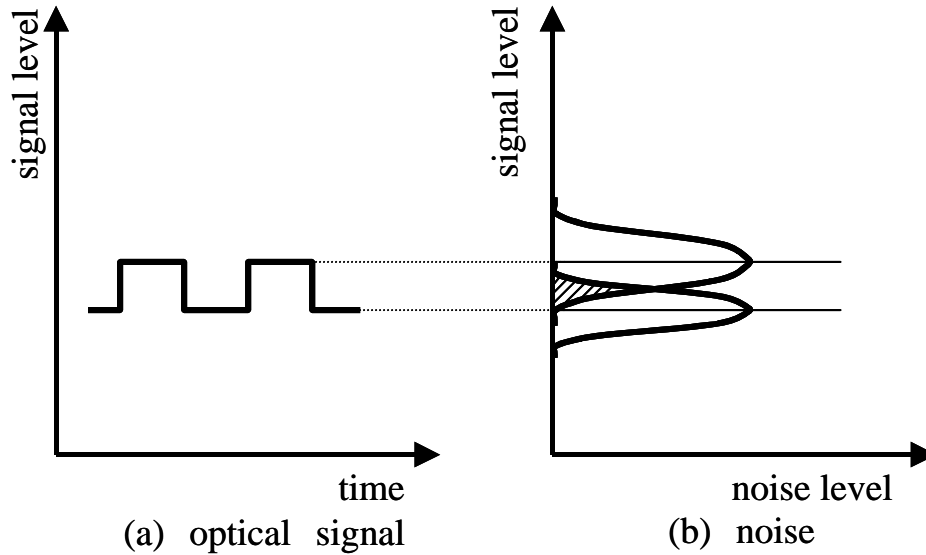


図 4.5 光信号とノイズ (小信号)

#### 4. 2. 2 基底の概念

ここでは、Y-00 暗号化で重要な役割を果たす基底について図 4.6 を用いて説明する。ここで、 $\alpha$  は光の振幅レベルとする。この振幅レベルに対して前述のように多値変調した値 ( $\alpha_1 \cdots \alpha_{2M}$ ) の組合せで、( $\alpha_1$  と  $\alpha_{M+1}$ ,  $\alpha_2$  と  $\alpha_{M+2}$ ,  $\cdots$   $\alpha_M$  と  $\alpha_{2M}$ ) のようなセットを構成する。この一つの組合せを基底という。したがって、基底の組合せ数が  $M$  であるので信号数は  $2M$  となる。正規受信者の受信時における信号振幅は基底の振幅 (例えば  $\alpha_{M+1} \cdots \alpha_1$ ) に等しく量子雑音の影響を無視できるため、共通の初期鍵により基底情報を持つことで正しい信号を得ることができる。これに対し、基底情報を持たない盗聴者は隣接間レベル (例えば  $(\alpha_{M+1} - \alpha_M) / (2M - 1)$ ) を識別する必要がある。それ故、隣接する信号振幅が小さいため両信号に付随する量子雑音分布が重なり、大きな S/N 劣化を生じ正しい信号を得ることは困難となる。



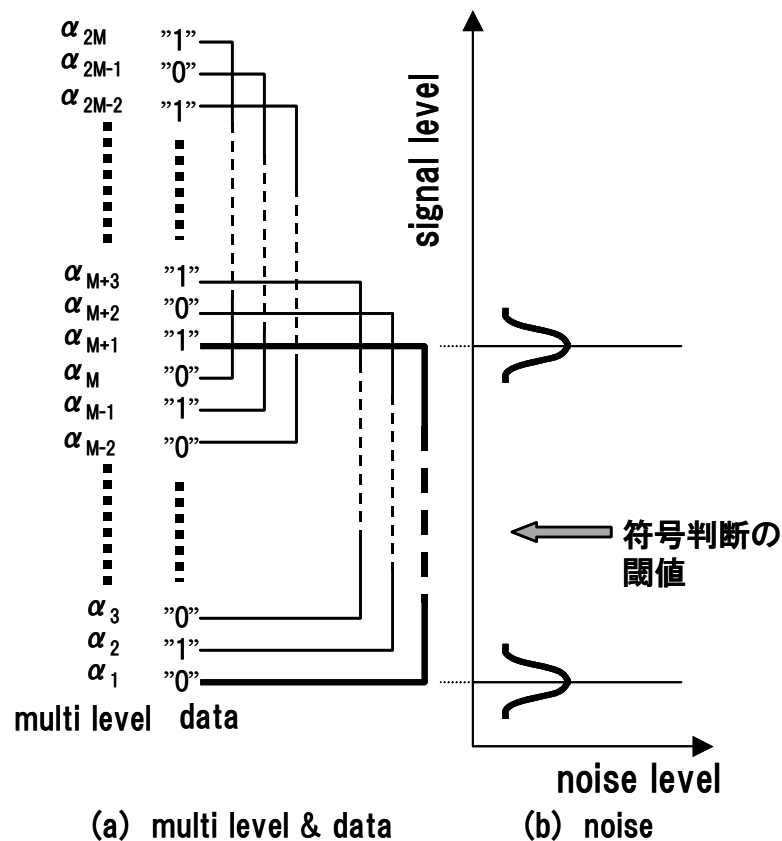


図 4.6 基底の概念

Y-00 方式の暗号化原理を図 4.7 (a) で示すように 8 値光強度変調方式の場合を例にとり説明する。ここで縦軸は光送信信号レベル、横軸は時間軸である。Y-00 方式では、多値化されたビットの異なる二つの光送信信号レベルの組合せにより” 1”、” 0” を決定しデータを伝達する。また、正規受信機ではこの暗号鍵に基づく組合セルール（基底）に応じて識別レベルを生成して” 1”、” 0” の判別を行うのでデータの再生に付いては、既存の 2 値伝送方式と同様に取り扱うことができる。図 4.7 (a) の場合の基底数は①～④の 4 種類となる。ここで、基底③を使って情報伝達を行う例について述べる。正規受信者は、時刻  $t_6$  のビットでは信号レベルが 2 (” 0”) または 6 (” 1”) の何れかを受信していることを共通鍵により予測できるので、最適な識別レベルを設定することが可能となる。基底の選択は初

期鍵を用いて伝送速度と同じ速度でビット毎にランダムに行われる。正規受信者は共通鍵を使い同じ速度で識別レベルを可変し、常に最適な識別レベルで受信信号の識別再生を行う。その時の雑音分布を図 4.7 (a) の右横に示す。縦軸が受信信号レベル、横軸が雑音レベルである。正規受信者は” 1”,” 0” 信号に付随して生じる雑音（ここでは、量子揺らぎのみを考える）に掛かることなく識別レベルを設定できるため、原信号を正しく再生することが可能となる。図 4.7 (b) は共通鍵を持たない盗聴者が盗聴する場合の受信信号の再生方法を示したものであり、同様の時刻  $t_6$  では基底を認識することはできない。仮に多値数を知ったとしても識別可能な 7 値の識別レベルを用意する必要がある。しかし、先程と同様に図 4.7 (b) 右横に示す受信信号レベルと雑音レベルで考えると信号間のレベル差が、図 4.7 (a) の 4 分の 1 になるため、雑音分布が所望の信号レベルに隣接する信号レベルと重なりが生じるので、S/N (信号電力対雑音電力比) が劣化し正しい信号検出が困難になる。この隣接信号間のレベル差を密にする程、雑音分布の重なりは強くなるので、盗聴者の信号レベルの S/N は極端に劣化し、正しいデータレベルの取得が益々困難となる。

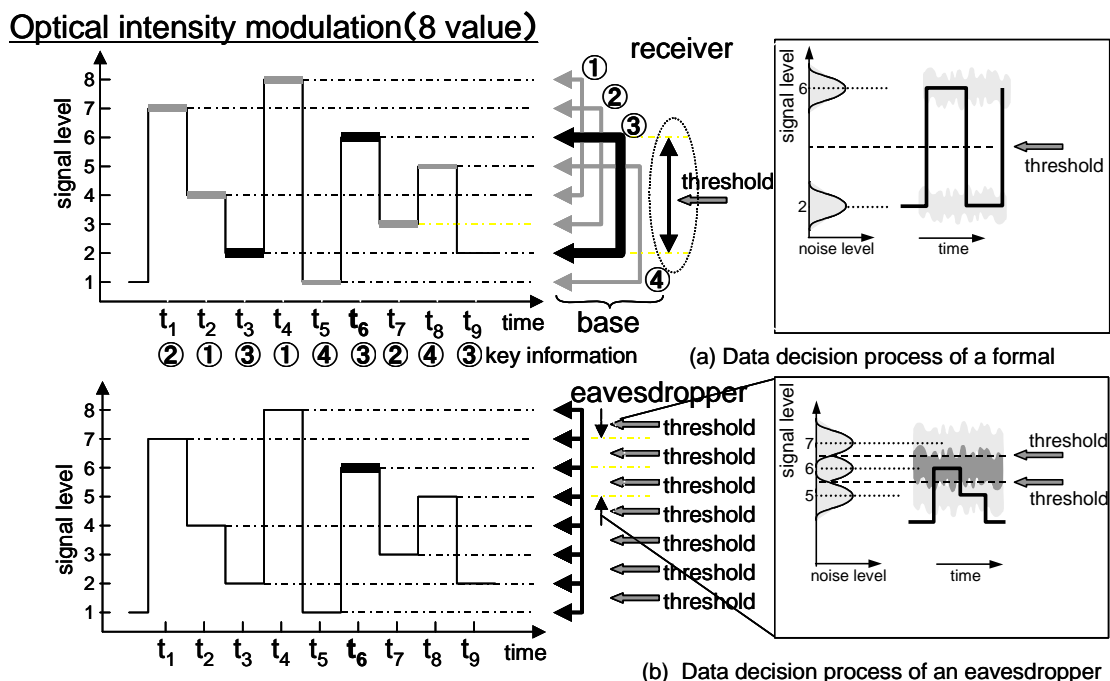


図 4.7 光強度変調型 Y-00 方式におけるの暗号化原理

すなわち、盗聴者は、この信号レベルを暗号解読のための情報として蓄積し、通信文である平文（暗号化する前の文）やランダム基底を作る擬似乱数生成器の鍵を計算処理により推測する。しかし、図 4.7 (b) の隣接間レベルを更に狭くすると、各レベルにおける雑音分布が重なるために正確なレベル検出が不可能になる。更に Y-00 方式では、多値の各レベルの隣接レベルに交互に平文情報（” 1”、” 0”）が対応させられているため隣接レベルの検出の S/N がゼロとなり、平文に対する安全性は情報理論的安全となる。しかし盗聴者は、平文ではなく、多値信号を多値信号として処理するために、ランダム基底を生成する擬似乱数生成器の鍵の解読が可能となる。したがって安全性の評価と強化は、多値信号に基づく信号処理能力の評価と、それをどのように劣化させるかという問題となる。これを考える上では真のレベルの量子雑音分布が、何番目までの隣接レベルと重なり合うかで安全性を決定することができる。

$$Q = \Gamma |k| / \log_2 M \quad (5)$$

上式は、その安全性を定量的に示した式である[27]。安全指数  $Q$  を大きくするには、 $\Gamma$ （隣接レベルの量子雑音が重なり合う範囲：識別不能領域）に制限がある場合、 $|k|$ （鍵長）または、 $M$ （基底数）を大きくする必要がある。装置の高速化を考慮すると、 $|k|$  を大きくすることは、回路の規模や動作速度を考えると好ましくない。また、同様に  $M$  を極端に大きくすることも同様な問題を抱えることになる。このため、現実の送信電力領域において、基本モデルでの量子雑音効果は小さいので、盗聴者の多値信号処理能力を制限するためには、種々のアイデアが必要となる。

今、各レベルの光子数  $N$  と安全を確保するための隣接間光子数  $\Delta N$  は以下の式で求められる。

$$\left. \begin{aligned} N_M &= P_M / (B \times h \nu) \quad (B : \text{伝送速度}, P : \text{光パワー}) \\ \Delta N &= N_M - N_{M-1} \\ \Delta N &\leq 0.36 \times \sqrt{N_M} \end{aligned} \right\} (6)$$

この式は、隣接間レベルの識別不能領域を 10 レベルまで量子雑音が影響するための条件と

なる[27]。Y-00 理論の報告によれば、多値信号の識別不能領域が 7~10 程度で、且つその範囲で一様なランダム化が実現できれば、分的全数探索以外に解読法が無いことが報告されている[27]。

#### 4. 3 Y-00 暗号化光送受信機の構成

##### 4. 3. 1 光送信部

図 4.8 に、Y-00 方式の有用性を検証するために試作した Y-00 暗号化伝送装置の根幹をなす光送信機のブロック構成を示す。この光送信機は入力データを暗号化する暗号化回路と LD (Laser Diode) 光を外部変調器 (External optical modulator) によりオン、オフさせて光ファイバ伝送路に送出する光変調部とから成る。入力データは初期鍵 (Seed Key) を用いた乱数発生器 1 (LFSR: Linear Feedback Shift Resister) でスクランブルされた後、多値変調器 (Code Modulator) に入力される。一方、ランニング鍵は同じ初期鍵を乱数発生器 2 によりスクランブルすることによって生成される。このランニング鍵が基底の選択信号の基となり、基底情報をランダムに拡散する拡散回路 (Random shifter) にて基底情報をランダムに拡散した後、最終的な基底を選択する信号を生成する信号セレクト回路 (Select signal) を介して多値変調器に入力される。多値変調器では、これらスクランブルされた入力データと基底選択信号とから多値変調信号が生成され、暗号化が行われる。次に、この暗号化された多値変調信号は外部変調器に送られ、電気-光変換される。この過程で、LD 光の量子雑音効果が付加され、物理的に完全な暗号化の処理が行われる。この後、多値変調された LD 光は光ファイバ伝送路に送出される。なお、乱数発生器 1 および 2 には同一品種の LFSR が用いられる。

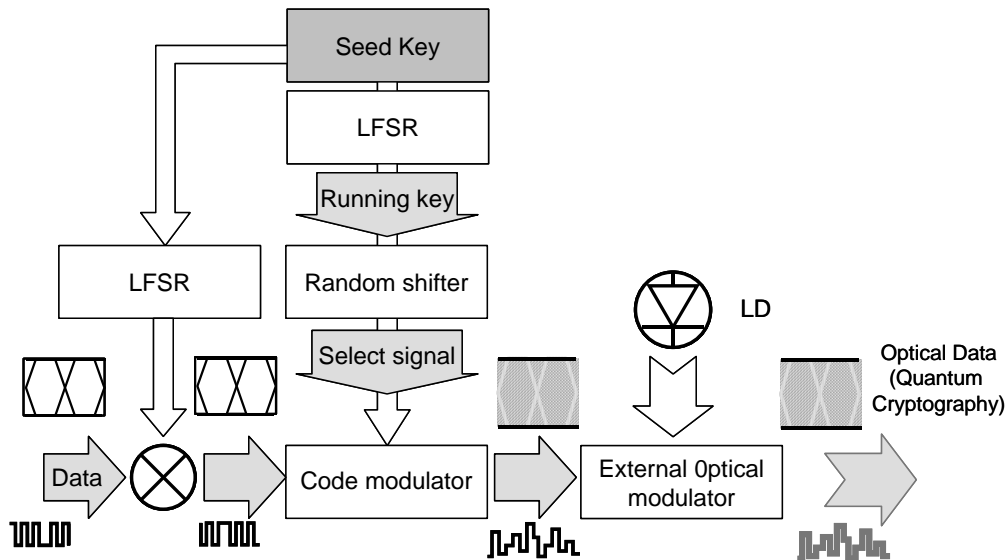


図 4.8 光送信機のブロック構成

#### 4. 3. 2 光受信部

図 4.9 に光受信機のブロック構成を示す。この光受信機は光ファイバ伝送路から入射される光信号を電気信号に変換する光-電気変換器と原データを再生する復調器 (Decoder) とから成る。復調器では、送信側で暗号化を施した処理過程とは逆の処理過程を経て暗号解除が行われ、原データが再生される。暗号解除処理は初期鍵 (Seed Key) を用いた乱数発生器 3 (LFSR: Linear Feedback Shift Register) でスクランブルされた信号と PD (Photo diode) で光-電気変換された受信信号と乱数発生器 3 で生成されたランニング鍵を基に受信データ識別レベル制御回路 (Threshold control)、信号セレクト回路 (Select signal) にて選択された基底信号とが多値復調器に入力される。多値復調器では、これら受信データと基底選択信号とから 2 値復調信号が生成される。次に、2 値復調信号に初期鍵と乱数発生器 4 で生成された信号とをミキシングしてデスクランブルすれば暗号が解除され、原データが復元される。なお、乱数発生器 3、4 には送信側で用いる乱数発生器 1、2 と同一品種

の LFSR が用いられる。

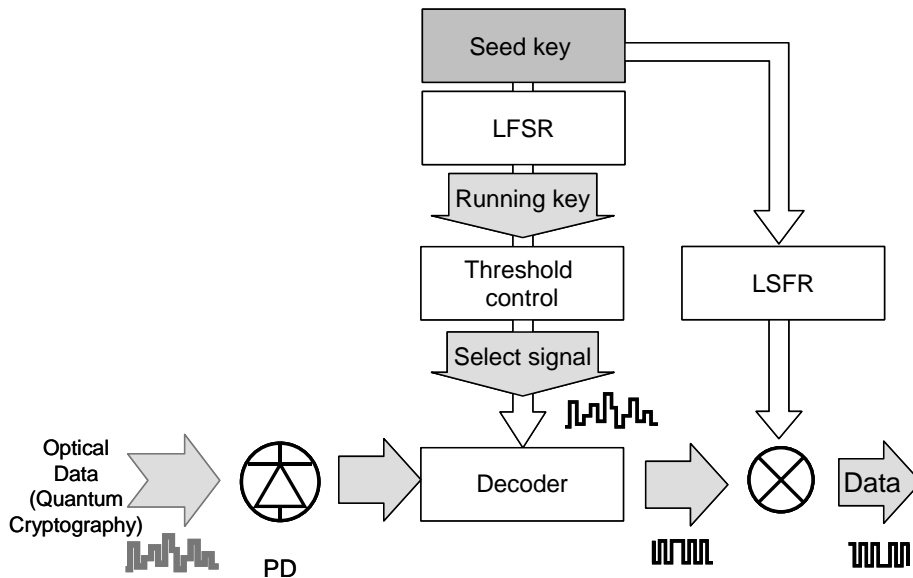


図 4.9 光受送信機のブロック構成

#### 4. 3. 3 多値変調／復調回路

多値変調回路の構成を図 4.10 に示す。この回路は信号セレクト回路から送られて来るセレクト信号コードに応じた多値レベルを生成する機能を持ち、基本的には簡易的なD/A 変換器とLD光を変調するLN (Lithium Niobate) modulator (リチウムナイオベイト光外部変調器) にて構成されている。この回路からの出力信号は光の外部変調器に入力され、電気-光変換される。今回の試作では、商用回線との互換性および暗号伝送の安全性を考慮し、伝送速度 2.5Gbit/s、セレクト信号 10 ビット (1024 値) に設定した。このため、10 個の外部変調器駆動回路 (DR0~DR9) が必要となり、それぞれの駆動回路の出力振幅に  $2^0, 2^1, 2^2, \dots, 2^9$  となるよう重み付けがなされる。次にこれら重み付けされた出力信号を全て組合せ加算することにより 1024 値の外部変調器駆動レベルが生成される

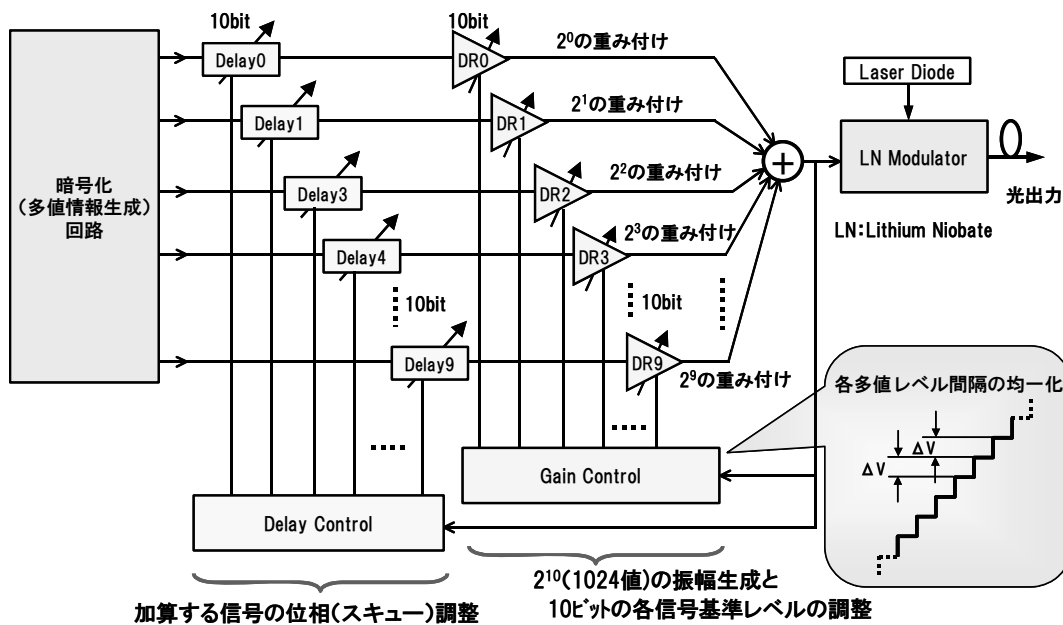


図 4.10 多値変調回路の構成

この加算時に各信号の位相が揃わないと波形劣化を起こすため、各ビットの多値情報生成信号は、各々の位相調整回路 (Delay0~Delay9) で調整を行い、加算後の多値信号波形の最適化を行っている。

図 4.11 に外部変調器として用いる LN (LiNbO<sub>3</sub>) 変調器の入出力伝達特性を示す。光信号の多値分割には線形性が求められるため、同図に示す線形性の良好な  $i$  を中心とした付近だけを使用している。このため、光出力信号振幅の最小値も十分光電力レベルは高く、消光比は 2dB から 3dB 程度となっている。それ故、通常の 2 値よりも正規受信者の受信感度は悪くなるが、信号の最大ピーク値と最小ボトム値の平均光子数の差が小さくなり、量子揺らぎの効果を均一にできる。また、消光比が 2dB から 3dB の中で 1000 値を超える多値分解を行うので隣接レベル間の光電力レベル差は非常に小さくなり量子揺らぎの効果を相対的に大きくとることができる。また、受信機における受信信号の復調に必要な識別レベルの生成も同様の回路を用いて実現できる。図 4.12 に復調回路の構成を示す。受信部で通常の光受信機には無い Y-00 量子暗号復調回路として重要な機能は高速 (伝送速度と等しい速度) 識別レベル制御機能であり、受信信号のビット毎に初期鍵を用いた識別レベル

の最適化を行う必要がある。更に、伝送距離による受信信号レベルの変動にも柔軟に対応する必要がある。本試作機では、受信信号のピーク値レベルの検出を行い、受信信号レベルの最大値と最小値（多値レベルの最大値と最小値）を検出して識別レベルの多値分割を行っている。識別レベルの最適受信条件は、送信機の変調部と同様に初期鍵からランニング鍵を生成し、前述の信号振幅から得た識別レベルから選択することにより決定される。

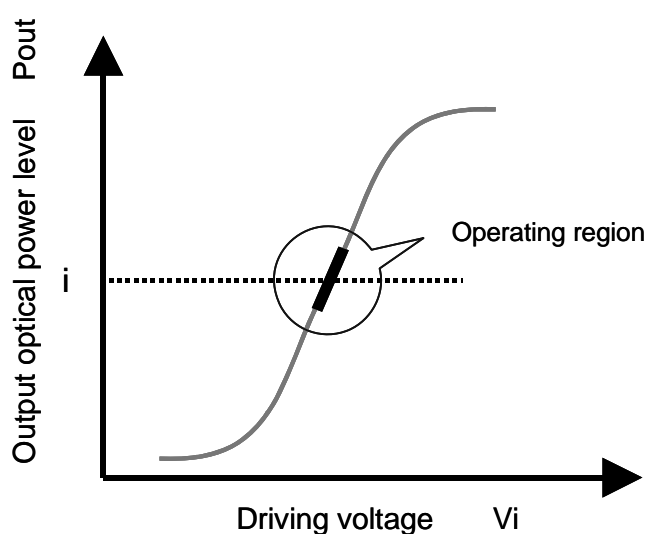


図 4.11 LN 変調器の入出力の伝達特性

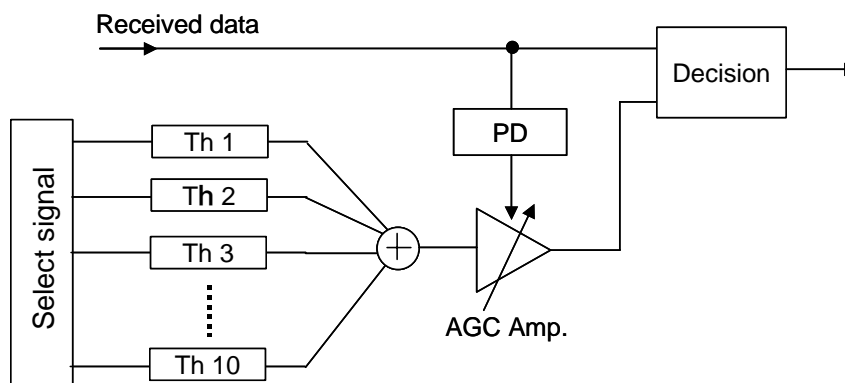


図 4.12 復調回路の構成



#### 4. 3. 4 多値変調部の詳細設計

前項で述べたように送信部および受信部では、共通に多値レベル生成回路が使われている。この回路の基本構成は、送、受信機ともに共通であり、図 4.13 のようになる。ディスクリット部品で組まれるこの回路の構成は、10 対（実際には、11 対であり 10 ビットの信号の内、信号振幅の重み付けで最大振幅を発生する 1 ビット分は、2 個の外部変調器ドライバ IC の出力をたし合わせて大振幅の信号出力を実現している。）の外部変調器ドライバ IC 出力信号を組合せ、これらの出力信号を加算し多値レベルを生成している。このレベル加算部は、高速化のため帯域に影響（制限）を与えやすい能動素子の回路（トランジスタ回路など）ではなく、比較的帯域制限を受けにくく帯域設計の容易な受動素子である抵抗加算によるシンプルな構成とした。抵抗加算部は、図 14 に示すように各ポート（10 ビット）からの信号のスキューを合わせるため、線路長を等しくする必要があり、各抵抗の一端を中心でまとめ放射線状に実装配置することで信号線路の等長化を図っている。

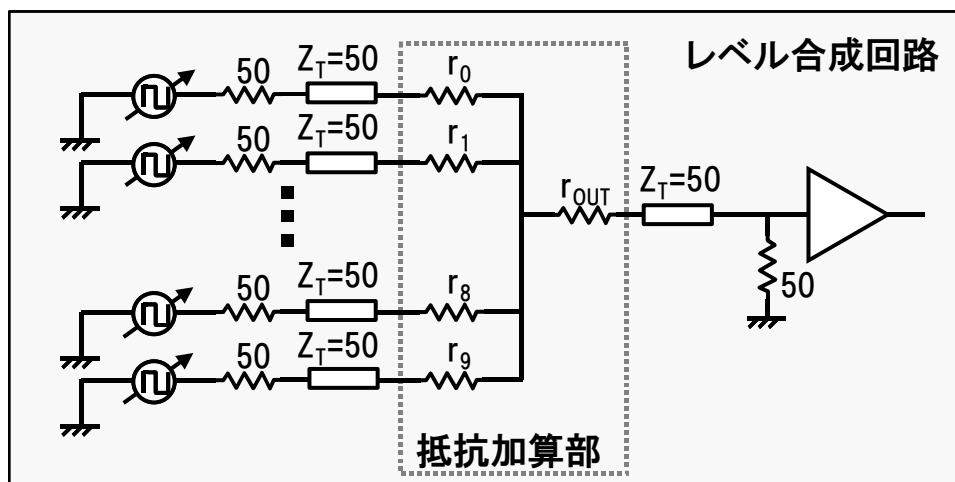


図 4.13 多値レベル生成回路

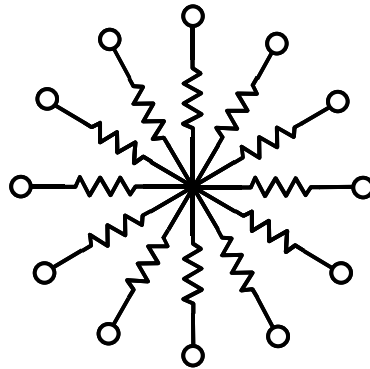


図 4.14 合成抵抗の等価回路

実際に設計した抵抗加算部を図 4.15 に示す。正 12 角形のセラミック基板の中心に薄膜のシート抵抗で集合抵抗を生成している。放射配置した伝送線路は、集積度を上げるため線路幅が微細化調整が可能なグラウンデッド・コプレーナラインを用いた  $50\Omega$  の伝送路を形成している。各ポートは出力インピーダンスが  $50\Omega$  の外部変調器ドライバ IC が接続され、出力ポートには、入力インピーダンスが  $50\Omega$  の LN 変調器を接続したときに、各ポートのインピーダンスが全て  $50\Omega$  になるよう中心の集合抵抗の形状を設計し決定している。

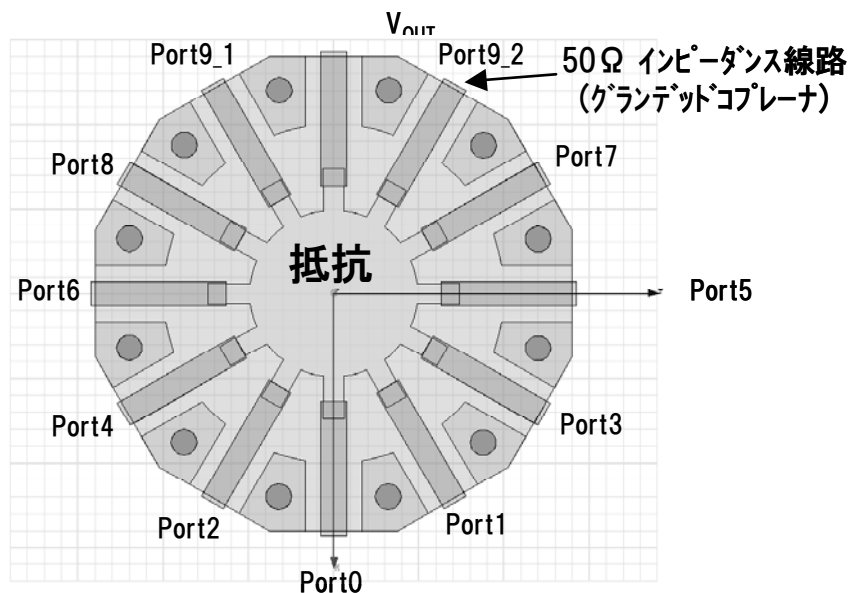
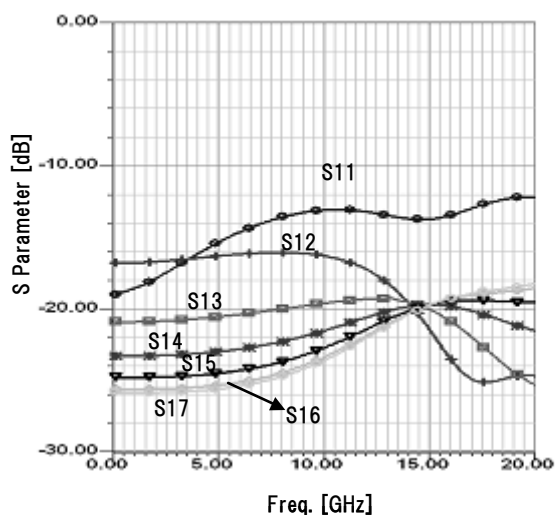
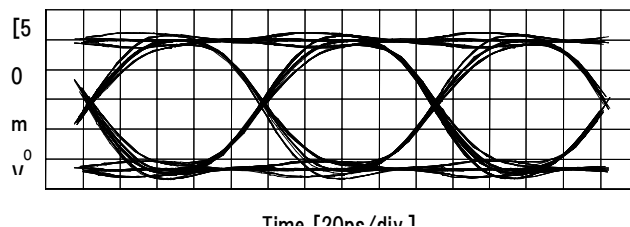


図 4.15 実際の基板パターン

この信号レベル合成部基板の詳細設計には高周波での設計の精度を向上させるために 3次元電磁界解析シミュレータを用いた。このシミュレーション結果を図 4.16 に示す。この図の (a) のように各ポートの小信号周特性 (S パラメータ) は、10GHz 以上で多少ピークを持つ帯域補償のかかった特性となった。また図の (b) の出力波形のような良好なアイパターンを得ることができた。



(a) 各ポートの小信号周波数特性



(b) 各ポートの波形の重ね合わせ

図 4.16 シミュレーション結果

#### 4. 3. 5 ランダムシフター

試作した伝送装置にはランダムシフターが使用されている。これは安全性の本質を高めるものではないが、盗聴者の信号識別に關与する条件付き確率を一様にする効果を持ち、理論的な安全性評価を可能にする役割を持つ。基本 Y-00 の構成においては、このランダム

化が理想的に実現されれば、その安全性の定量化は、前述の式(5)で与えられる[15][18]。

アメリカでは、実用化に向けて非線形のフィードバックシフトレジスタを採用しているが、日本では短い鍵長で済ませるため、線形フィードバックシフトレジスタ(LFSR)とランダム化を組み合わせる方法が提案されている[27][30]。その基本概念は、4.2.1項で説明した量子雑音の効果を更に有効にするために量子雑音の効果を拡散させ、より暗号解読を困難にするというものである。本研究では、それらの中で、比較の実効性のあるものを実際に実装することを目的としている。ここで採用するランダム化の構成を図4.17に示す。入力したデータ(平文データ)は、盗聴者の暗号文単独攻撃と既知平文攻撃を等価にするために開発されたOSK(Overlap Selection Keying)[21][26]で情報の正負がランダムに切り替えられる。一方、基底選択信号は、受信機と共通の初期鍵(Seed Key)を線形フィードバックシフトレジスタ(LFSR1)によりランニング鍵(Running Key)を生成し、これをKeyed DSR部で多値信号の条件付き確率が一樣になるように拡散を行い、基底レベルの選択信号(Basis Level Select Signal)を生成する[31]。更に不規則マップ(Irregular Mapping)部により、高速相関攻撃に対する免疫性を持つ多値レベル選択信号(Multi Level Select Signal)を生成する[32]。この選択信号を用いて前述のOSKされたデータに変調をかけ、電気/光変換を行うためのドライブ信号を作成する。

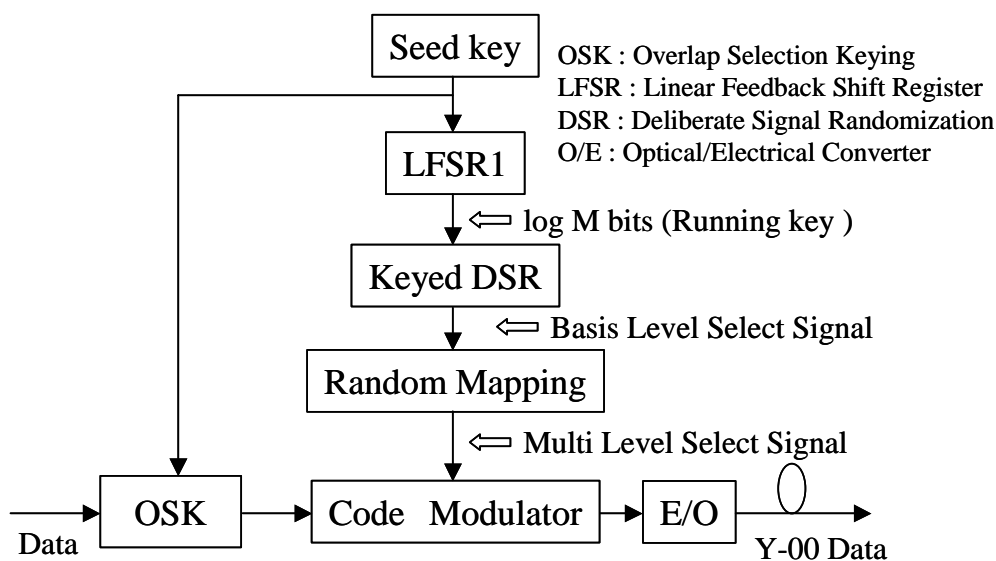


図 4.17 Y-00 暗号化の構成

### (1) OSK (Overlap Selection Keying)

OSK とは異なる情報 (” 1”、または、” 0”) を光の ” High”、または、” Low” レベルに任意に振り分け盗聴者が受信レベル検出を行えたとしても信号の情報が ” 1” であるか ” 0” であるか解読することを困難にする手法である[30]。

OSK の構成を図 4.18 に示す。OSK を実現するために送信機では乱数発生器 (LFSR3) を用いた方式によって、1 タイムスロット毎に 1 ビットの正/負論理ビット (Logic Bit) を生成する。ここで、正/負論理ビットとは、情報の ” 1” と ” 0” を光強度の ” High” と ” Low” に対応させた場合が正論理、情報の ” 1” と ” 0” を光強度の ” Low” と ” High” に対応させた場合が負論理として、これらの論理を選択し決定するビットである。論理の選択は、情報ビット (Data) とこの正/負論理ビットの排他的論理和 (XOR) を取ることによって実現している。つまり、この正/負論理ビットが ” 0” のときは正論理、” 1” の場合は負論理とする。

OSK の回路構成は、一般的なストリーム暗号と同様な方式をとるが、その目的と効果は異なる。基本 Y-00 では、隣り合う基底の符号は、1 つおきに ” 1”、” 0” を入れ替えているが、このままだと盗聴者は、1 レベルおきに ” 1” もしくは ” 0” に的を絞り符号を推測することができるため、多値数 (基底数) を 1/2 にした場合と同様の安全性になってしまう。そこで 1 ビット毎に符号を変化させることにより暗号解読の困難な度合いを維持することができる。

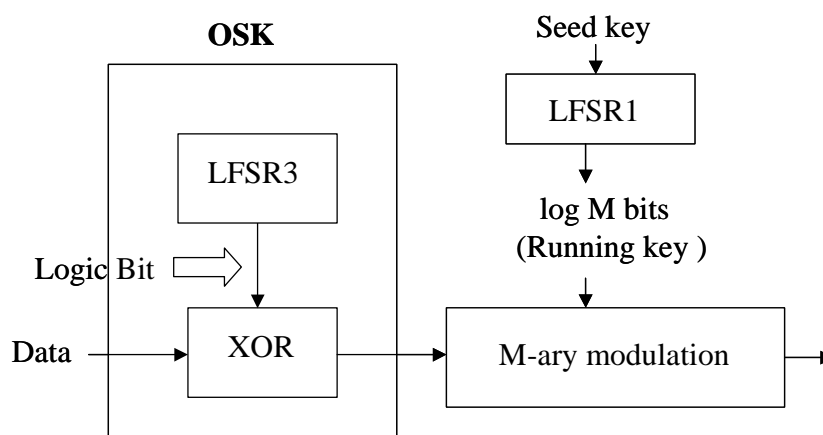


図 4.18 Y-00 に対する OSK の構成

(2) Keyed DSR (Keyed Deliberate Signal Randomization)

Y-00 の基底選択において多値信号の条件付確率を一様にするのが暗号理論的に重要であることが指摘されている。それを実行するために、当研究のグループが提案した Keyed DSR を用いる[31]。Keyed DSR は、安全性を直接強化するものではなく、盗聴者が多値信号を受信する際の量子雑音の条件付き確率を均一化するための補正技術である。この手法は前項で述べた盗聴者の S/N 劣化の効果（隣接レベル間量子雑音の重なり）を広域に一様に拡散させる役割を果たす。この仕組みを図 4.19 で説明する。

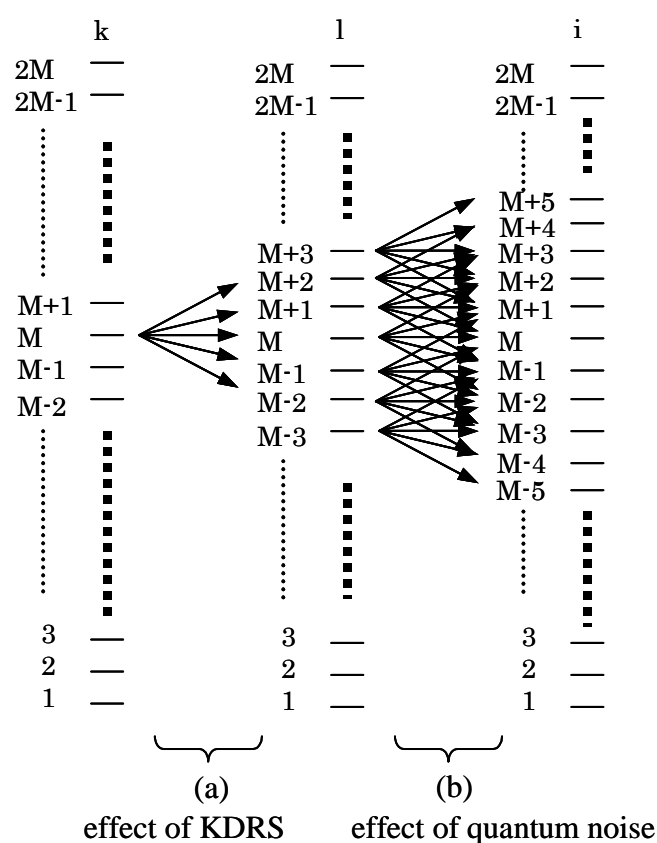


図 4.19 ランダムシフターによる拡散のしくみ

光強度変調を用いる Y-00 方式では、多値のレベルの中から Seed Key で選択された基底レベルが、隣接レベルの量子雑音分布と重なり合い、レベル検出に誤りを発生させている。理想的には多値の信号レベル全体を一様にできることが望ましいが、その場合は正規受信者の受信感度劣化を招くため、通信が困難になる。そこで Keyed DSR では、基底選択信号 (Running Key) の下位数ビット (今回の試作では、正規受信者の受信感度と隣接レベル間パワーを考慮して 3 ビットとした) を LFSR2 でスクランブルすることにより、意図的に基底レベルをランダムに±数レベル (今回の試作では 2 レベル) の範囲でシフトさせている。この状態を図 4.20 (a) に示す。このときの Keyed DSR を用いて拡散させたことによる  $i$  の真値を  $l$  のレベル測定で誤る確率を  $P(l|i)$  とする。更に図 4.21 (b) の様に拡散された個々のレベルの分布に対して、各レベルにおける量子雑音の分布関数  $P(k|l)$  が一様に配置されるため、真の基底レベルを誤る条件付き確率  $P(k|i)$  は、以下の式のようになる。

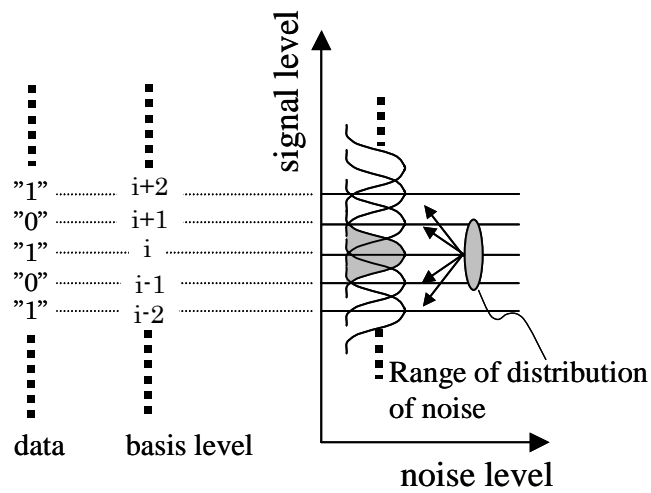
$$P(k|i) = \sum_l P(k|l)P(l|i) \quad (7)$$

そのときの正規受信者の受信感度に及ぼす影響は、多値レベル数が  $2M$  値、信号全振幅が  $P_{2M}$ 、Keyed DSR によるレベルの拡散を  $\pm n$  とすると信号レベルの劣化分  $P_{KDSR}$  は次式のようになる。

$$P_{KDSR} = 2(P_{2M}/2M) |n| \quad (8)$$

ここで、試作した装置を例にとると、 $2M=1024$  値、 $n=\pm 2$  であるからこの場合、信号の全振幅パワーの  $1/256$  程度の劣化であり、正規受信者にとっての影響は小さい。

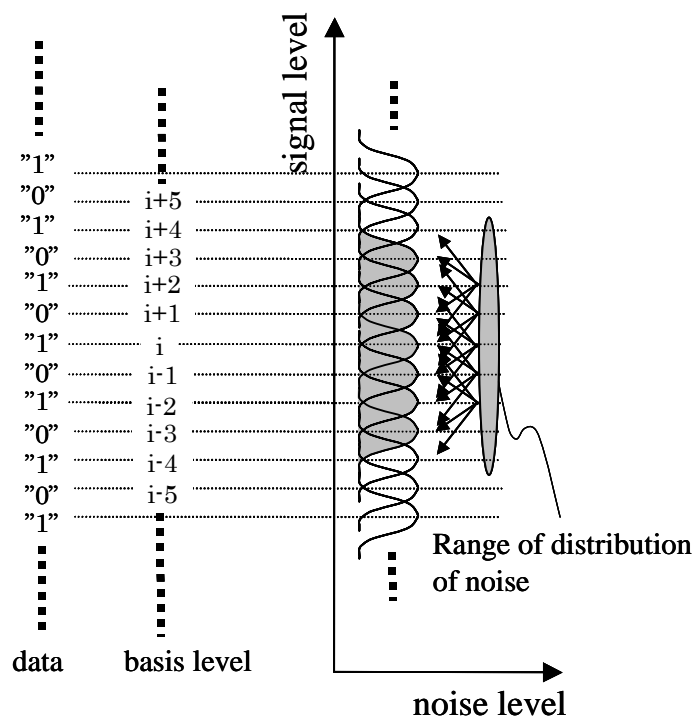
Keyed DSR を量子雑音の分布の観点から説明すると以下のようになる。図 4.20 は、Keyed DSR をかけないときの信号レベル  $i$  の隣接レベルへの影響の範囲を模式的に表した図である。この図では、量子雑音の効果が自分のレベルを基準に±2 レベルまでしか影響を及ぼすことができない。このため盗聴者は、基底選択信号の誤り確率の偏りが起こるので、基底選択信号の一部を推測できる可能性が高くなる。そこで、図 4.19 のように基底の選択を決定付ける基底選択信号 (Running Key) に Keyed DSR を施すことにより図 4.21 のようにノイズは拡散される。このため基底選択信号の誤り確率分布の偏りが少なくなるため多値信号としての Running Key の推定は非常に困難になる。



(a) data & basis level

(b) noise

図 4.20 ノイズの拡散 (Keyed DSR 無)



(a) data & basis level

(b) noise

図 4.21 ノイズの拡散 (Keyed DSR)



Keyed DSR を実現するための回路構成を図 4.22 に示す。Seed Key を用いて生成された First running Key は、乱数発生器 (LFSR2) の出力を加算することで keyed DSR を行う。First running Key はこの乱数により基底レベルの選択信号の下位数ビットをスクランブルすることで、図 4.21 のような量子雑音の拡散を実現する。

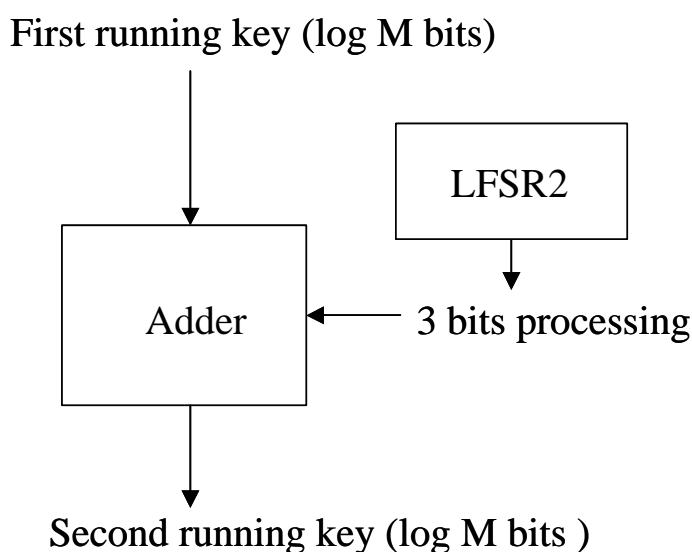


図 4.22 Keyed DSR の構成

### (3) 不規則マッピング (Irregular mapping)

基本モデルでは隣り合う基底を表す多値信号のビット表現においてビット誤り位置が不均一になるため、鍵長が短いときには高速相関攻撃が有効となる場合がある[33]。アメリカでは鍵長を 4000 ビット、或いは、非線形のフィードバックシフトレジスタを採用しているので問題がないが、我々のように短い鍵長モデルでは問題となる。しかし、そのような高速相関攻撃を無効にするためにはビット誤り位置が均等になるようにすれば良い。短い鍵長の場合でも高速相関攻撃に対する免疫を持たせる不規則マッピングが開発されている[32]。ここではそれを採用している。これによって、部分全数探索以外に解読不可能となる。図 4.23 にその概念を示す。基底に対応する多値レベルのマッピングにおいて、全く不規則に基底を配置させ、これをテーブル化して送信者—正規受信者間で共有する。この手法を

用いると、物理的に量子雑音の範囲が同じでも隣り合う基底を表す多値信号のビット表現においてビット誤り位置が均等に拡散される。このため、多値信号をビット表現に戻したときにビット誤り率の不均一さをを用いた高速相関攻撃が機能しないことになる。図 4.24 に不規則マッピングの構成を示す。基底レベルの選択信号 (Basis Level Select Signal) は、選択信号変換部 (Select Signal Converter) でマッピングテーブル (Mapping Table) を用いて不規則マッピングを実行する。

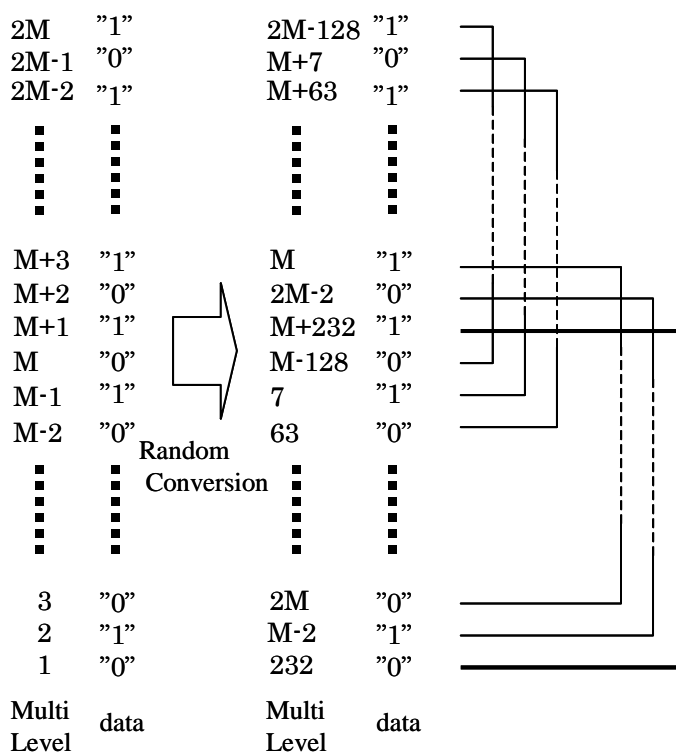


図 4.23 不規則マッピング

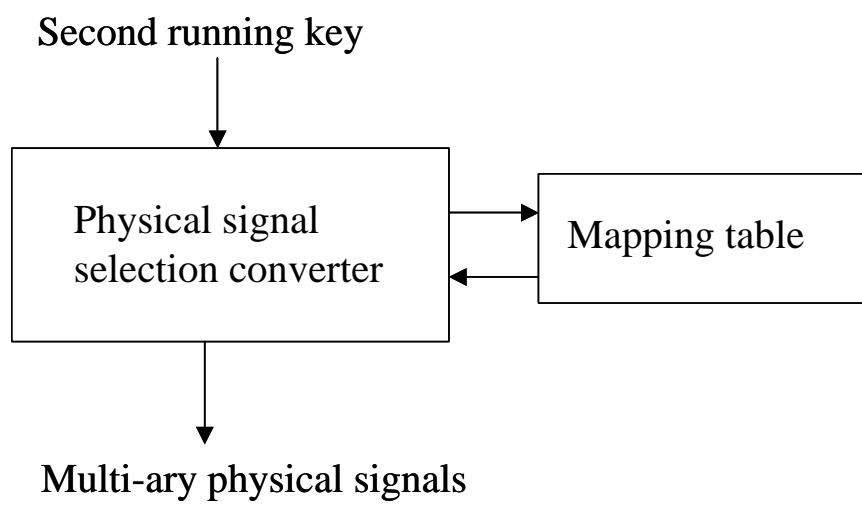


図 4.24 不規則マッピングの構成

#### 4. 4 Y-00 光送信機、受信機の試作結果

##### 4. 4. 1 基本特性

Y-00 の基本特性を検証するために、Y-00 暗号化光送信機と受信機の試作および実験を行った。図 4.25 に試作した Y-00 暗号化光送受信機の外観を示す。送信機、受信機ともに大きさは、それぞれ 19 インチラックに搭載可能で、高さは 2U (Unit) であり、STM16/OC-48 に対応する電気入出力用と Y-00 暗号回線用光信号インタフェースを有している。主要特性は、表 4.1 に示すように、伝送速度は 2.5Gbit/s で、暗号化のための基底数を 128、光出力信号の出力レベル数を 256 とした。平均光出力電力は 0dBm である。なお、この光送信機、受信機の試作は、初期段階の基本特性を確認するため多値数は 256 値 (基底数 128) で行った。

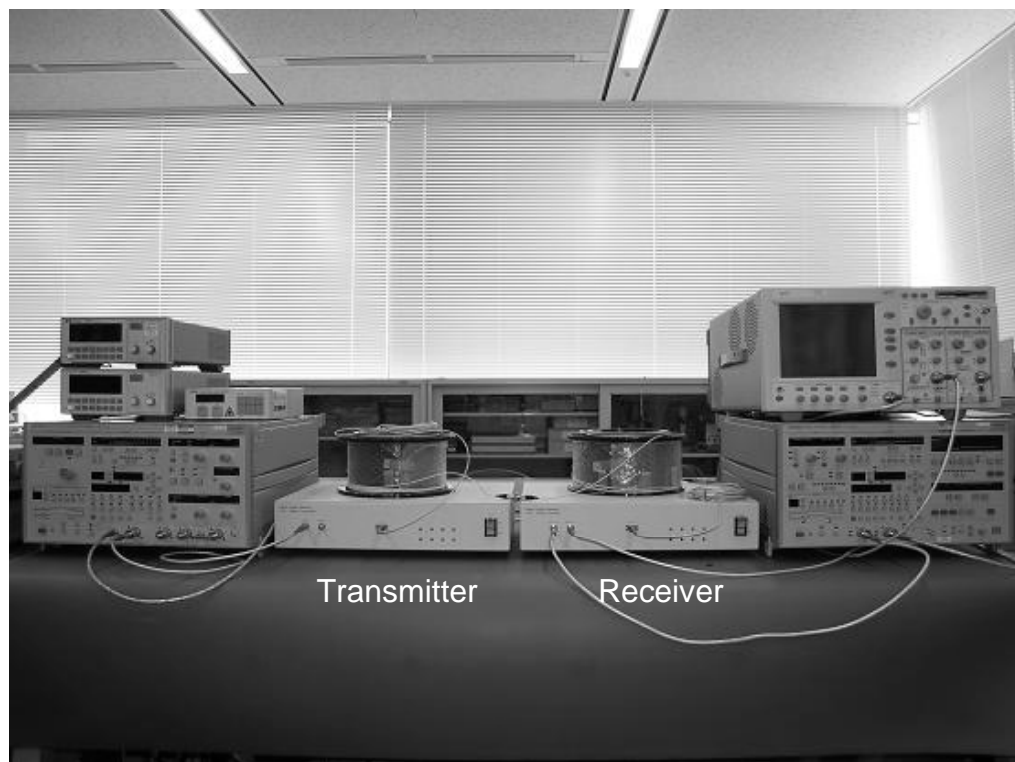


図 4.25 試作した光送受信機の外観と測定系

表 4.1 試作光送受信機の主要特性

item	unit	result
Data rate	G bit/s	2.48832
Transmission distance	km (w/o amp.)	50
Output power	dBm (ave.)	0
Number of basis (Number of levels)	- (-)	128 (256)

#### 4. 4. 2 安全性の評価

提案したY-00方式の安全性を検証するために、正規受信者と盗聴者に対する符号誤り率特性の評価を行った。図 4.26 にそれら符号誤り率特性の評価結果を示す。光送信機の出力信号を1:1の比率で2分岐し、片方を正規受信者の、もう一方を盗聴者の受信機に分配した。また、実験は256値（基底数128）で行い、量子揺らぎの効果を確認しやすいようにランダムシフターは用いていない。盗聴者の受信機には正規受信者の受信機と同等性能のものを用いて、受信感度を測定した。盗聴者の符号誤り率は $3 \times 10^{-1}$ 程度であり、受信電力を増大させても符号誤り率は飽和する傾向を示し、正しい信号レベルの識別ができないことが分かる。強力な盗聴方法として鍵の全数探索がある。これは盗聴データを想定できる全ての鍵数と同数データを並列コピーし、全ての鍵を個々に当て嵌め、一斉に解析作業を試み相関を取れる共通鍵を見つけ出す方法である。Y-00方式の場合、盗聴者がデータを取得（光/電気変換）した時点で量子雑音によりデータは誤りを生じるので、電気データをコピーして全ての鍵を当て嵌めても解析することはできない。そこで、光ファイバを分岐して、光の状態のコピーしたデータの取得が必要になる。分岐した光信号は、想定できる個々の鍵を持つ受信機を鍵と同数並べて一斉に解析される。しかし、光ファイバの分岐数を多くすると、受信データのS/Nは劣化し誤り率が増加する。このためコピー（分岐）の数と受信機の符号誤り率の関係を明らかにすることにより安全性を確認することができる。

図 4.27 に多値数と符号誤り率特性を示す。光送信機からの出力信号を 1:1 に分岐した後、更にカプラーを用いて並列コピー数の分岐を行い、受信信号の符号誤り率特性を測定した。使用した試作光送受信機の初期鍵の生成数（コピーすべき分岐数）は約 1030 個であるのに対して、盗聴者の分岐数は 500 程度で誤り率は増大し  $5 \times 10^{-1}$ （究極の誤り率=0.5）に漸近していくため盗聴者は信号レベルの検出が不可能となる。なお、これらの実験において盗聴者の受信機は何れも正規受信者と同等な性能の受信機を用いて測定を行った。

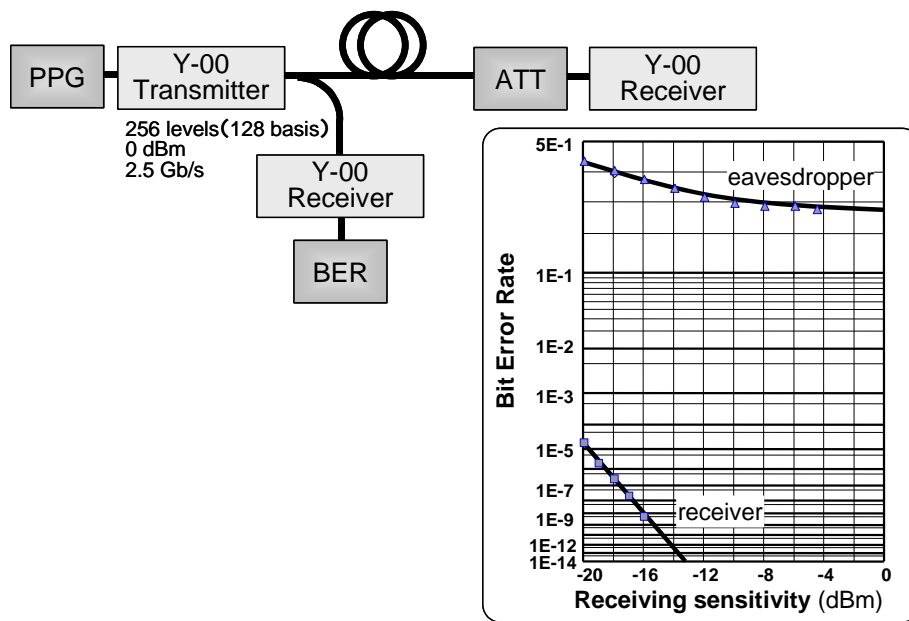


図 4.26 盗聴者に対する受信感度

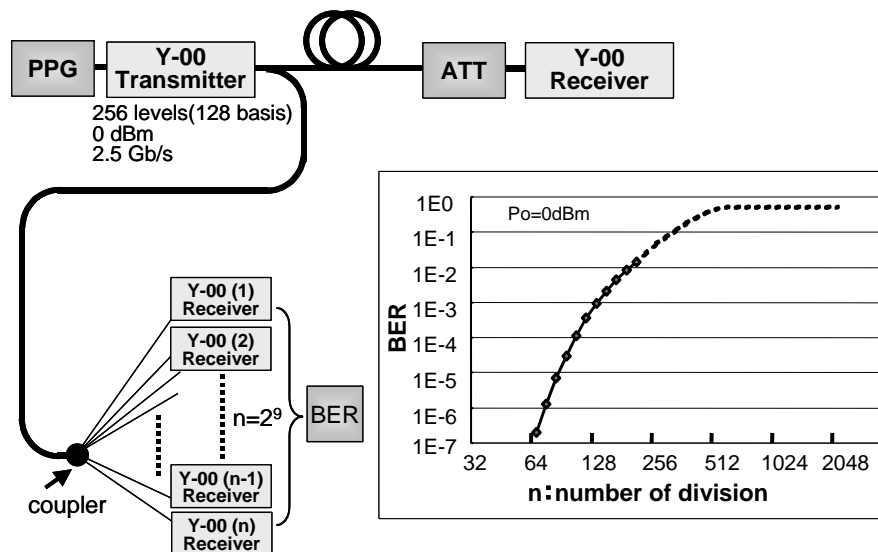


図 4.27 並列コピー盗聴の受信感度

#### 4. 5 Y-00 トランシーバの開発

##### 4. 5. 1 Y-00 暗号化変調回路

Y-00 暗号化伝送装置の中核を成す送信部暗号化変調回路の構成を図 4.28 に示す。入力された 2.5Gbit/s (STM-16) の平文データはデマルチプレクサ (DMUX) 16 分離 (156Mbit/s × 16) され、ロジック処理が可能なデータ速度に並列展開される。ここで、平文データから CDR (Clock Data Recovery) 回路によって抽出された自己同期に必要な Clock 信号が分離動作に使われる。Y-00 の伝送では、同期処理や制御等を行うための情報を基の信号に付加する。このため FIFO (First Input First Output) 回路で 156Mbit/s から 167Mbit/s のデータ速度に変換した後、Framer でフレーム処理を行い、同期信号等で必要な情報を付加する。この信号には、4. 4. 4 項で述べたように OSK 処理が施される。この信号は 16 : 1 のマルチプレクサ (MUX) で多重化され、2.7Gbit/s の主信号が生成される。

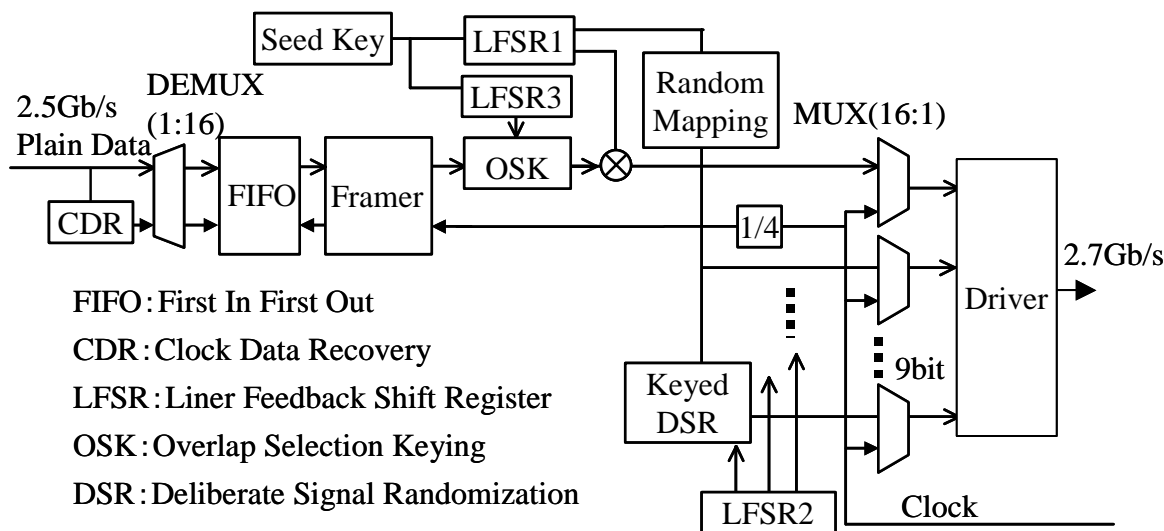


図 4.28 Y-00 送信部の暗号化回路の構成

一方、多値レベルの選択信号は、以下の手順で行われる。まず、LFSR1 を用いて Seed Key から Running Key を生成する。その後に Random Mapping を施すことで、基になる基底選択信号が生成される。更にこの選択信号には、下位 3 ビットに対して LFSR2 を用いた KDSR 処理がおこなわれ、2.7Gbit/s の多値レベル選択信号が 9 ビット生成される。2.7Gbit/s の主信号と同じ 2.7Gbit/s、9 ビットの多値レベル選択信号は、それぞれのドライバ (Driver) 回路により、重み付けおよび加算されて、多値レベルの基底信号が生成される。この最終段の処理は、D/A コンバータと同様な処理となる。ここで生成された基底信号を用いて光外部変調器を駆動することにより Y-00 暗号化信号を生成できる。

#### 4. 5. 2 多値変調回路

図 4.29 に多値変調回路の構成を示す。多値変調部では、前項で説明した暗号化された 9 ビット+1 ビット、合計 10 ビットの信号から 1024 値の多値レベルの信号を生成する。10 ビットの信号は、それぞれ位相調整回路 (Delay0~9) を通り、利得可変増幅器 (DR0~9) にてビット毎に重み付けされる。その後、この 10 ビットの信号を組合せ、アナログ加算することにより 1024 値の光のレベルに対応した光外部変調器の駆動信号が生成される。光外部変調器は、LN (Lithium Niobate) 変調器を用いている。LN-変調器では、LD の CW (Continou Wave) 光を駆動信号により変調をかけ、Y-00 暗号化光信号を実現している。



多値レベル間隔は、常に等間隔な線形性が要求されるので、各ビットの出力信号のレベルおよび位相は、出力信号を監視・誤差検出して負帰還フィードバック制御（Delay and Gain control）を行うことにより、多値信号のレベル間隔が均一で、且つ、線形性が保てるように制御できる構成になっている。また、LN-変調器の駆動レベルの範囲は LN-変調器の消光特性（余弦カーブ特性）で線形性の最も良い最大出力の 1/2 近傍を中心に、最大消光比が 3dB 以下となる様に設定している。受信感度を犠牲にし、消光比を小さく抑える理由は、量子雑音が生子数の平方根に比例するため、多値信号の各レベルで均一な量子雑音分布を得ようとするとき出力レベルの最大値と最小値とで光子数の差を小さくする必要があるためである。

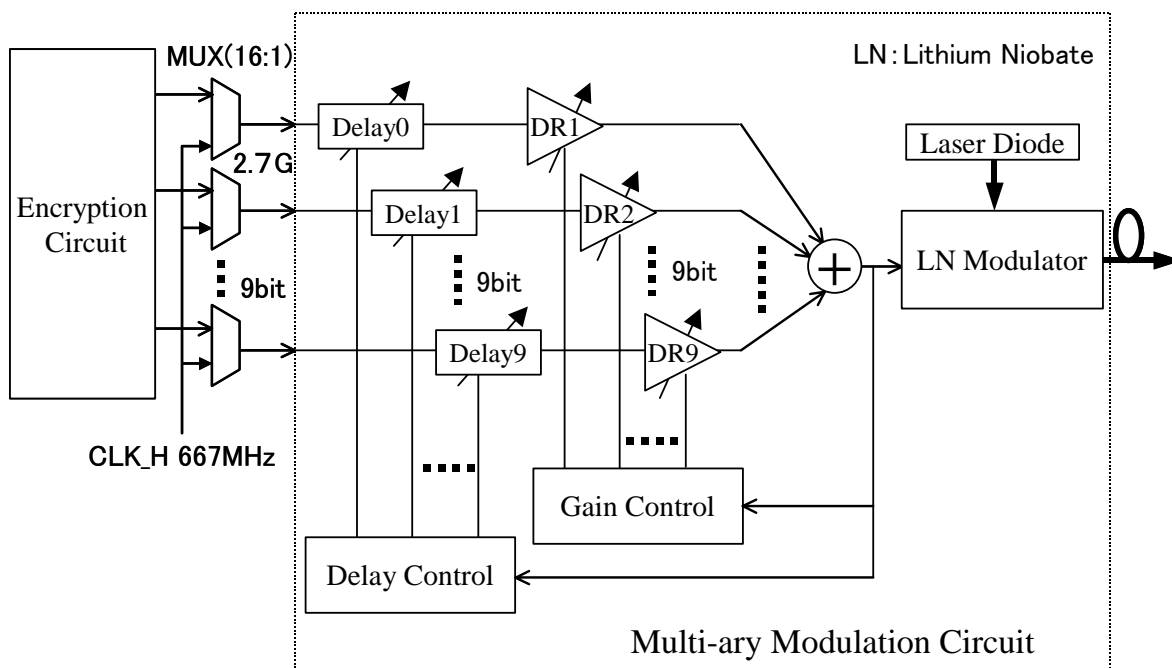


図 4.29 多値変調回路

#### 4. 5. 3 受信機 (復調回路)

図 4.30 に Y-00 受信機の複合化回路の構成を示す。初期鍵および OSK で使用する鍵は共通鍵として、また不規則マップの共通テーブルも受信機にも装着し用いている。復号部 (Decoder) は、基本的に送信機の暗号化部と同様な回路構成となる。しかし受信部で Keyed DSR の復号処理は行わないので復号部からは、10 ビットの Y-00 複合化信号 (閾値選択信号) を出力する。閾値制御部 (Thresh Control) では、1 ビット毎に信号識別用の最適なレベルとタイミングの閾値選択信号を生成する。この閾値のレベルとタイミングは、AGC 増幅部 (AGC Amp.) と閾値制御部で最適化調整を行う。また、復号部では、Y-00 複合化のためのビット同期と鍵同期の確立を行っている。

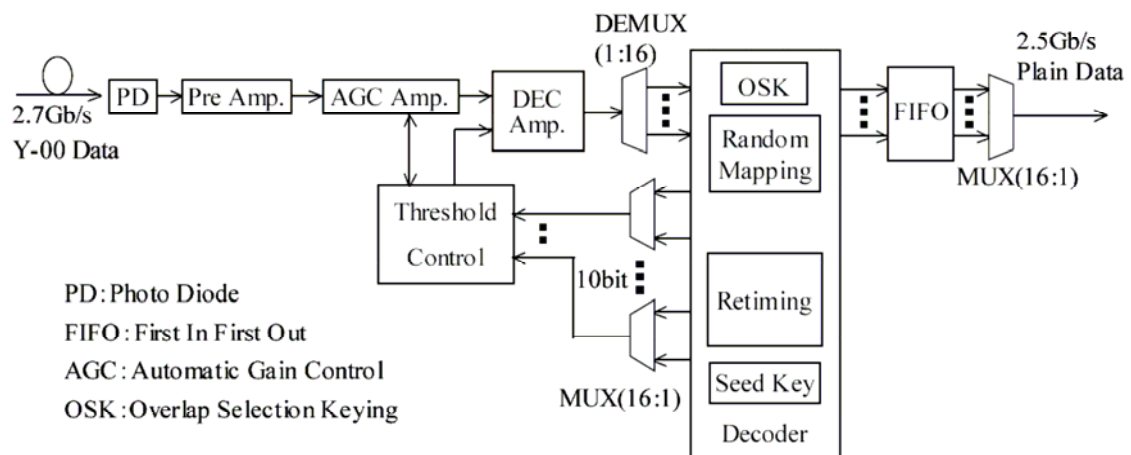


図 4.30 Y-00 受信部の復号化回路の構成

#### 4. 5. 4 トランシーバの試作結果

試作した Y-00 トランシーバの主要特性を表 4.2 に示す。先に試作した送信機および受信機同様に、伝送速度は、標準規格である STM16 および OC-48 に準拠した 2.48832Gbit/s であり、無中継時の伝送距離は 50km 以上とした。基底数は 4 倍の 512 であり、多値数は 1024 値である。

表 4.2 Y-00 トランシーバの主要特性

item	unit	result
Data rate	G bit/s	2.48832
Transmission distance	km (w/o amp.)	50
Output power	dBm (ave.)	0
Number of basis (Number of levels)	- (-)	512 (1024)

また、装置の大きさは、前回試作した送信機、受信機と同様で 19 インチラック対応の 2U サイズである。しかし、今回試作した装置は、トランシーバであり、1 台の装置に暗号化送信機と受信機を 1 台に集約した構成になっている。また、このトランシーバは、伝送実験等での使い勝手を考慮し、モデムやメディアコンバータのようなイメージで使えるように入力側は、標準規格である STM16 および OC-48 の光入出力インタフェースを持ち、Y-00 に光-光変換して利用することが可能になっている。図 4.31 に試作したトランシーバの外観を示す。

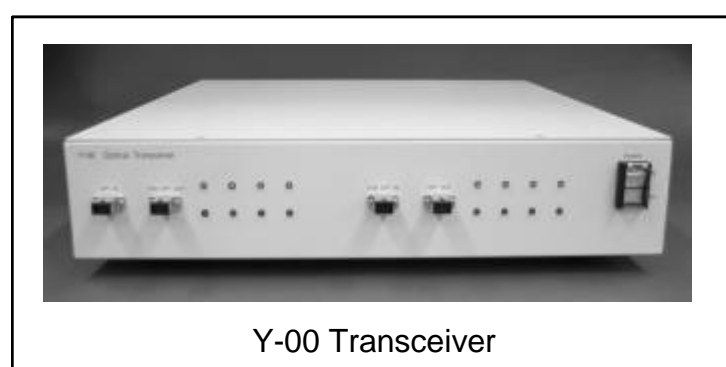


図 4.31 Y-00 トランシーバの外観図

図 4.32 に正規受信者の Back to Back での受信感度特性を示す。平均光出力が 0dBm のとき

に、誤り率（ビットエラーレート：BER） $10^{-12}$ のときに、-15.3dBmとなった。

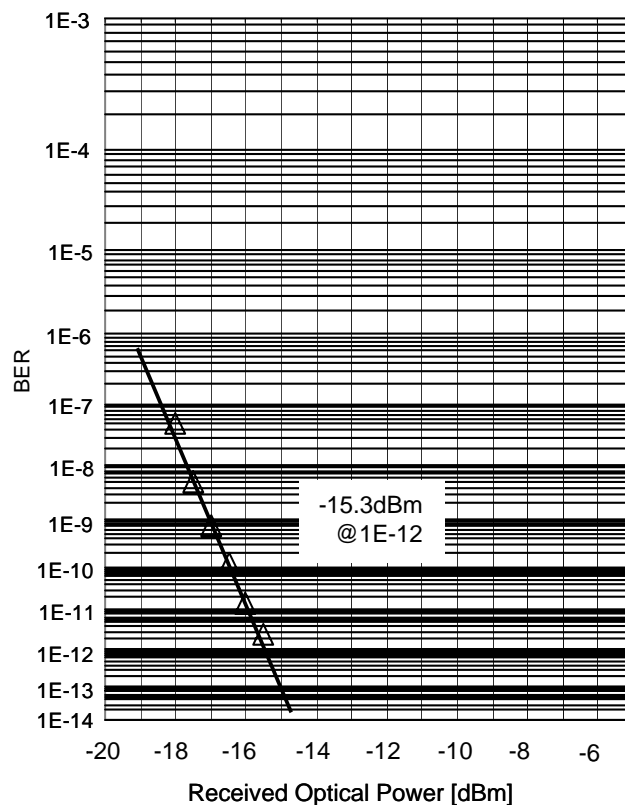


図 4.32 正規受信者の受信感度特性

#### 4. 6 伝送実験

次世代ネットワーク等で期待されている新しい安全性の高い通信技術の確立の第一ステップとして、提案したY-00方式の有用性、並びに、現在広く利用されている商用ネットワークへの適用可能性を検証するために、試作したY-00暗号化光送受信機を用い、既存の商用回線を使って伝送実験を行った。図 4.33 に伝送実験を行ったネットワークの構成を示す。中継区間数は4、1中継当たりの距離は48kmで、3台の光ファイバ増幅器（EDFA；Erbium Doped Fiber Amplifier）を中間中継器として用い、総伝送距離192km、伝送速度2.5Gbit/s、符号誤り率 $10^{-12}$ のY-00暗号伝送が可能であることを確認した。ここで、1中継区間の伝送路損

失が 15dB程度と大きかったため、送信側にブースター用、受信側で光前置増幅用として市販の光ファイバ増幅器を導入した。以下に、その他のアプリケーション伝送実験で検証した詳細内容を纏めて示す。

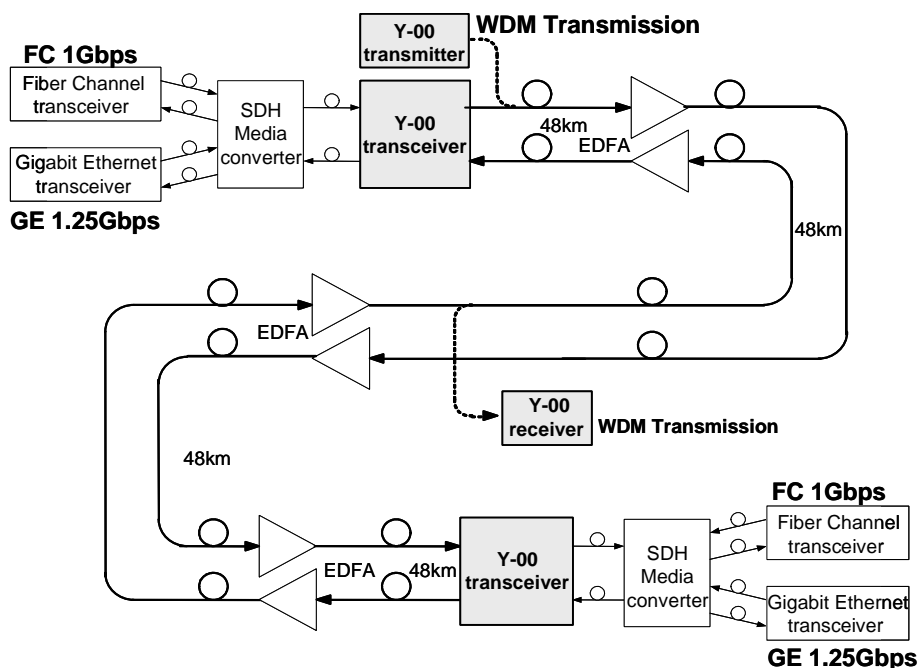


図 4.33 Y-00 方式の現場実証試験用ネットワーク構成

(1) SDH (Synchronous Digital Hierarchy) フレームの伝送実験

Y-00 光送受信機 3 中継、192km の Y-00 暗号伝送において、2.48832Gbit/s の PRBS (Pseudorandom Binary (Bit) Sequence) 31 段信号、SDH フレーム信号の双方において符号誤り率  $10^{-12}$  以下のエラーフリーの暗号化信号伝送を確認した。

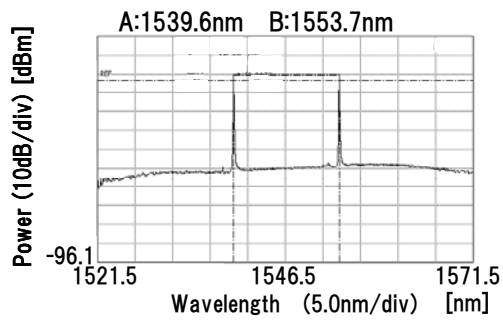
(2) ファイバチャネル、ギガビットイーサの伝送実験

SDH メディアコンバータを介して、1Gbit/s ファイバチャネル信号と 1.25Gbit/s イーサネット信号を多重化した後、Y-00 方式による暗号化を施し、192km 伝送の実験を行なった。Y-00 平文としてファイバチャネル、GbE (Gigabit Ethernet) パケットを載せた OC-48 信号を使用して暗号伝送を行い、マルチサービス機器試験機にてファイバチャネルの正常

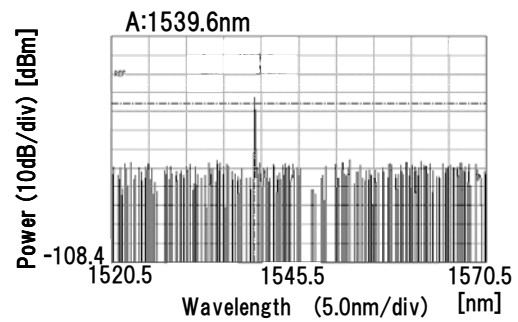
動作、マルチポート・ネットワークデバイス試験機にて IP パケットの正常動作を確認した。また、FC (Fiber Chanel) 測定器で観測した伝送系のレイテンシは、1.29ms であり、そのうちファイバで  $960\ \mu\text{s}$  ( $5\ \mu\text{s}/\text{km} \times 192\text{km}$ )、残り  $330\ \mu\text{s}$  が Y-00 光送受信機と使用したメディアコンバータ、ファイバチャネルスイッチのレイテンシの合計となる。

### 3) WDM 伝送実験

図 4.34 に WDM 伝送実験を行った時の波長配置と Y-00 光送受信機のスペクトルを示す。同図 (a) は使用した波長は  $1.5396\ \mu\text{m}$  および  $1.5537\ \mu\text{m}$  の 2 波長であり、同図 (b) は波長  $1.5396\ \mu\text{m}$  の光フィルタ透過後の信号スペクトルで、 $1.5396\ \mu\text{m}$  の信号が選択されていることが分かる。図 4.35 (a) および (b) に、それぞれ試作光受信機の受信信号および再生出力信号の波形を示す。受信信号には受信増幅器の熱雑音が重畳されるので受信 S/N が若干劣化するが、総 S/N は送信 S/N 符号でほぼ決まるため、劣化量は無視できる。また、正規受信者の受信感度を図 4.36 に示す。各条件を考慮して計算をおこなったシミュレーション値と実測値を比較すると符号誤り率  $10^{-12}$  において back-to-back で実測値が  $-18.2\text{dBm}$ 、シミュレーション値が  $-18.6\text{dBm}$  であり、192km の伝送後では、実測が  $-19.4\text{dBm}$ 、シミュレーション値が  $-19.7\text{dBm}$  となりほぼ一致した結果を得ることができた。図 4.37 に伝送実験における光送受信端局の外観を示す。上り回線、下り回線用として 2 台の Y-00 光送受信機が設置されている。2.5Gbit/s 光伝送特性評価装置 (パルス・パターン・ジェネレータ、符号誤り率測定器) から入力される PRBS=31 段の信号列は Y-00 光送受信機にて暗号化され、現場に敷設されている商用回線に送出される。商用回線では中間中継器 (光ファイバ増幅器) 3 台を経て相手方の Y-00 光送受信機にて受信され、暗号解読の後原信号が再生される。反対側の回線も同様な伝送処理が行われる。

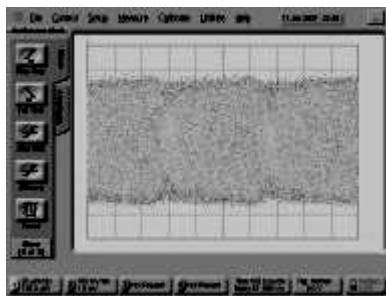


(a) WDM wavelength spectrum

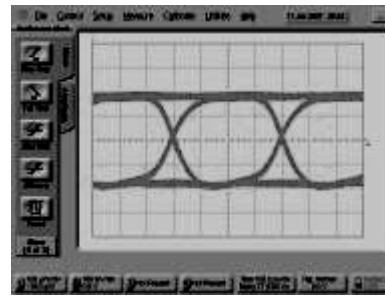


(b) Y-00 transceiver spectrum (After the WDM filter)

図 4.34 WDM 伝送時の波長配置および Y-00 光送受信機のスペクトル



(a) Y-00 ciphertext data



(b) Decryption data

図 4.35 伝送波形

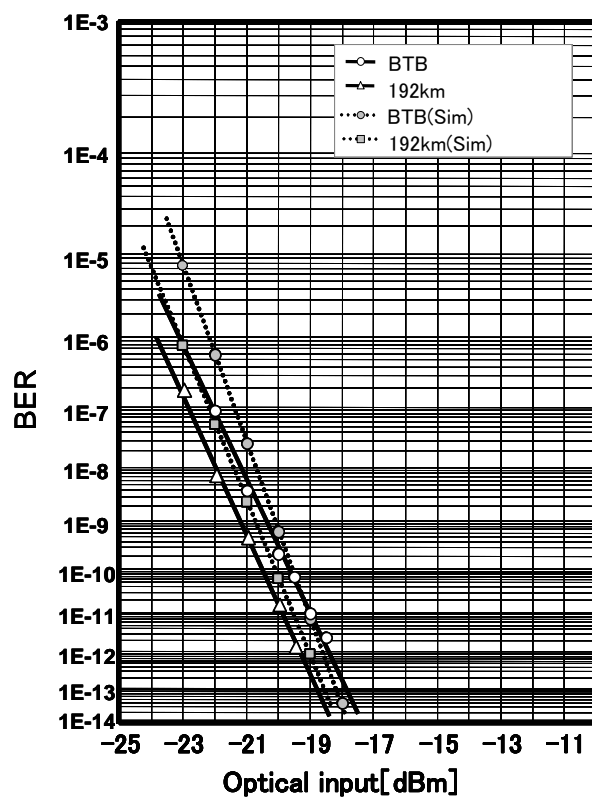


図 4.36 Back-to-back および 192km 伝送時の符号誤り率特性



図 4.37 伝送実験用に試作した Y-00 光送受信端局の概観



## 4. 7 10Gbit/s Y-00 伝送装置の開発

### 4. 7. 1 高速化の検討

前項で報告してきた 2.5G/s 伝送装置を基に、更なる高速化のため 10Gbit/s の実現に向け開発を始めている。これまで開発してきた 2.5G/s 伝送装置の一部は 10Gbit/s への展開を想定して基本設計行ってきた。4. 3. 4 項の基板設計においても 10Gbit/s 伝送を意識している。しかし、Y-00 受信機の暗号複合部では、通常の光通信と違い閾値を共通鍵から生成した多値情報を基に伝送速度と等しい速度（1 ビット毎）で閾値レベルを移動させる。このため受信側では、通常の光通信の識別再生部よりも広帯域な設計が必要となる。特に多値レベル生成部は精度の高い設計が必要となるため、DAC (Digital / Analog Converter) 機能を集積化した DAC-IC として開発を行った。

IC 化を行うにあたり適切な IC プロセスを選定する必要がある。3 章でのシステム LSI 開発での経験を生かし選定を行った 10Gbit/s 動作に余裕が持て、且つ LN 変調器を直接駆動することが可能な 50Ω 負荷で出力振幅 (2.5V<sub>p-p</sub> 以上) を得るためのデバイスの耐圧を考慮すると、前章のシステム LSI 開発で採用した SiCMOS プロセスでは不可能であり、SiGe の BiCMOS を適用することとした。表 4.3 に使用したトランジスタプロセスの基本デバイスパラメータを示す。

表 4.3 0.25 μ m UIISO/SOI SiGe BiCMOS プロセス

項目	単位	Min.	Typ.	Max.	備考
Emitter size	μ m <sup>2</sup>		0.2×1.0		
h <sub>FE</sub>	-	150	300	1000	V <sub>CE</sub> =1V, I <sub>CE</sub> =10 μ A
BV <sub>CB0</sub>	V		2.5		I <sub>B</sub> =1nA, I <sub>CE</sub> =10 μ A
BV <sub>CE0</sub>	V	9			
f <sub>T</sub>	GHz	72	90	100	V <sub>CE</sub> =2V
f <sub>max</sub>	GHz		180		

$f_T=90\text{GHz}$ 、 $f_{\text{max}}=180\text{GHz}$  (Typ.) であり  $10\text{Gbit/s}$ の信号を扱うには十分であり高速動作に期待が持てる。また、耐圧も $BV_{\text{CE0}}\geq 2.5\text{V}$ であり大振幅の出力に対応できる。

#### 4. 7. 2 回路設計

##### (a) 回路構成

図 4.38 に多値信号生成部である  $10\text{Gbit/s}$ 、10 ビット DAC IC のブロック図を示す。回路は大きく分けて 8 つのブロックで構成されている。DAC に入力された  $10\text{Gbit/s}$ 、10 ビットの多値生成信号は、最初のブロックであるデータラッチ回路に入力される。この回路は入力データを基準クロックによりラッチすることにより、配線遅延などにより発生した 10 ビットの入力信号間のスキューを補正し、後段のブロックに送る役割を果たしている。タイミング補正されたデータ上位 4 ビットがサーモメータデコーダ、下位 6 ビットがダミーサーモメータデコーダに送られる。サーモメータデコーダは入力されたバイナリ信号をサーモメータ信号に変換する回路であり、DAC の性能に影響を与えるグリッチがバイナリ信号のタイミングのズレにより生じるので、これを回避するために本方式を採用した。上位 4 ビットをサーモ信号に変換しているのは上位 4 ビットが、特に出力信号レベルの変動（推移）が大きいためグリッチの発生量も大きくなり、多値変換後の波形に対するグリッチ雑音の影響の方が下位ビットよりも大きいためである。変換ビット数はグリッチ量と回路面積・消費電力とのトレードオフで 4 ビットと決定した。本回路のようにサーモメータとバイナリを組合せる方式は、一般にセグメント方式と呼ばれている。

ダミーサーモメータデコーダは、上位 4 ビットのサーモメータデコーダ回路で発生する遅延を補償するため、同様な回路遅延を下位 6 ビットに与える回路である。

次段のプリドライバ回路はサーモメータ信号、バイナリ信号を同じタイミングでカレントステアリング回路に送る役割を果たしており、次段のトランジスタの入力容量が流れる電流に応じて違いため、それぞれに応じて前段バッファの負荷駆動能力を調整している。カレントステアリング回路は、実際にデジタル信号をアナログ信号に変換する回路である。変換方法は、 $R\cdot 2R$  ラダー抵抗網と OP アンプの基準電圧により生成された重み付け電流をデジタル信号のビット重みと関連付け、各電流源スイッチの ON・OFF によりその重みに対応した電流を抵抗に流すことによりアナログ多値信号に変換する。本回路では、次段の LN 外部変調器を駆動する必要があるため、設計目標の最大出力振幅を  $2.5\text{V}$  とした。この

ためカレントステアリング回路の電流スイッチに流れる電流はトータル 100mA となる。分解能 10 ビットのうち、上位 4 ビットがサーモメータ信号、下位 6 ビットがバイナリ信号であるのでサーモメータ回路の電流スイッチ 1 個に流れる電流は、合計出力電流 100mA の 1/16 の 6.25mA とする。下位 6 ビットでは 1/16 の 6.25mA を更に 1/2、1/4、1/8、1/16、1/32、1/64 と重み付けを行った。

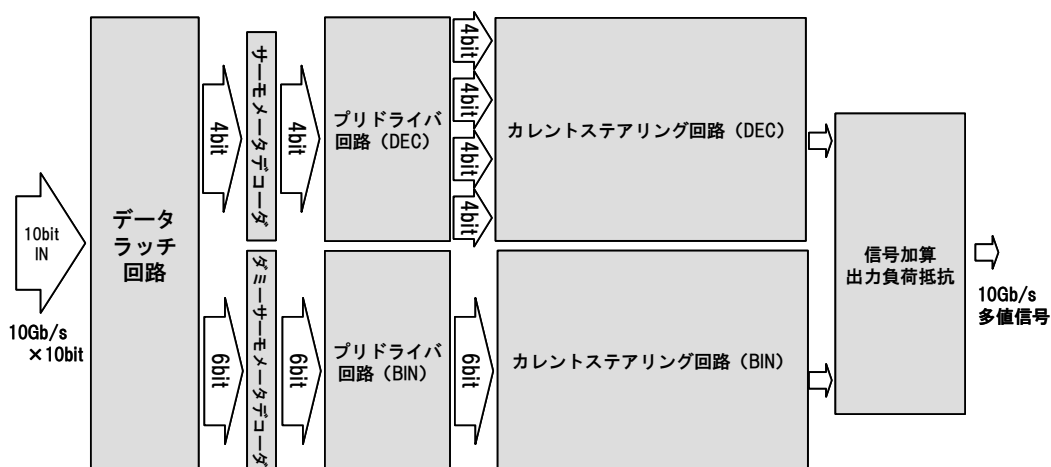


図 4.38 10Gb/s 10 ビット DAC のブロック図

### (b) 高速化の検討

DAC の動作速度は出力電圧を 1 ビットのビット間隔である既定時間 (10Gb/s の場合、100ps) 内に、入力のデジタル信号で決定される電圧値まで到達させる必要がある。今回の回路方式ではカレントステアリング回路及び出力部 (信号加算出力負荷抵抗) の構成が動作速度を決める大きな要因であるため、カレントステアリング部および出力部の基本回路は、高速動作が可能な差動増幅器 (電流スイッチ) で構成することにした。以下この回路で採用している差動回路の高速化の検討について述べる。

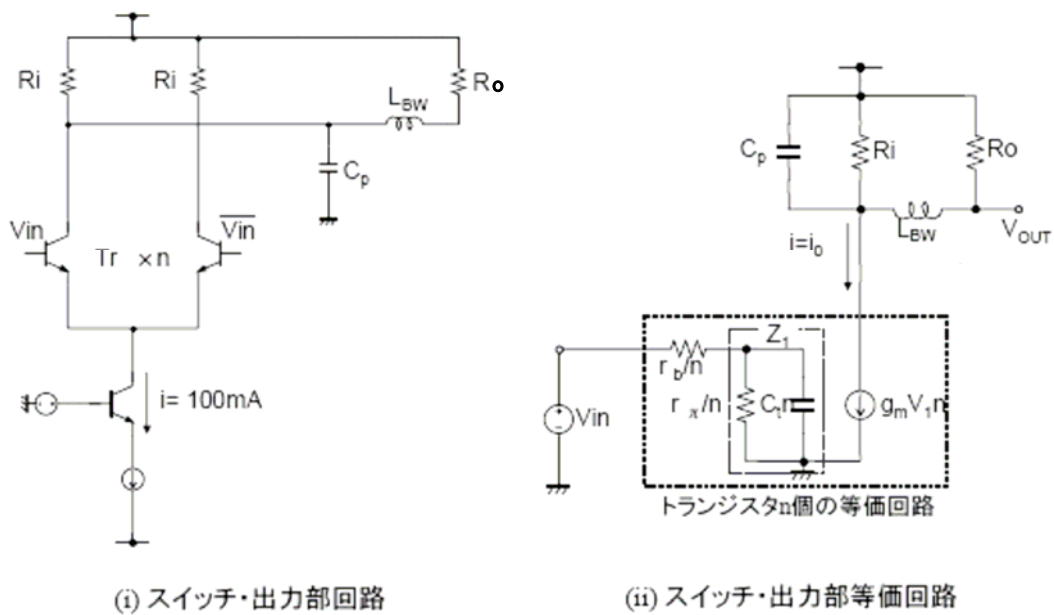


図 4.39 スイッチ出力部回路及び等価回路

DACの高速化を図る上で出力信号波形の立ち上がり時間の律束要因を特定するために出力部等価回路の解析を行った。図 4.39 に差動電流スイッチ・出力回路及び等価回路を示す。(i)の回路は、上位 4 ビットのカレントステアリング回路で使用する 21 対の差動回路を考え、この方式で最も厳しい動作、即ちカレントステアリングを構成している全てのスイッチが同時にOFFからONに切替わり、100mAの電流を切り換え 2.5Vppの出力振幅を想定し、差動電流スイッチに使用する全てのトランジスタを $Tr \times n$  ( $n$ : トランジスタ総並列数)として検討した。 $R_i$ はIC内部の出力負荷抵抗 (信号加算出力負荷抵抗)、 $R_o$ は次段のLN外部変調器の入力抵抗、 $C_p$ は出力部寄生負荷容量、 $L_{BW}$ は、ボンディングワイヤのインダクタンスである。

(ii)の図は、出力部の等価回路を表している。小信号等価回路では、トランジスタのエミッタ接地と置き換え考えることができる。ここでは $r_b$ をベース抵抗、 $r_x$ を入力抵抗、 $C_t$ はミラー効果を考慮した入力容量とする。伝達関数を求めるためにまずは、入力 $V_{in}$ と出力抵抗に流れる電流 $I_o$ との関係を考える。図の (ii) の破線で囲まれた合成インピーダンスを $Z_1$ と

し、トランジスタ $n$ 個の入力インピーダンスを $Z_{in}$ とすると以下のように表すことができる。

$$Z_1 = \frac{\frac{r_\pi}{n} \times \frac{1}{sC_t n}}{\frac{r_\pi}{n} + \frac{1}{sC_t n}} = \frac{1}{n} \left( \frac{r_\pi}{1 + sr_\pi C_t} \right) \quad Z_{in} = \frac{r_b}{n} + Z_1 = \frac{1}{n} \left( r_b + \frac{r_\pi}{1 + sr_\pi C_t} \right) \quad (9)$$

電流変化に関する $V_1$ は、以下のようになる。

$$V_1 = \frac{\frac{1}{n} \left( \frac{r_\pi}{1 + sr_\pi C_t} \right)}{\frac{1}{n} \left( r_b + \frac{r_\pi}{1 + sr_\pi C_t} \right)} V_{in} = \frac{\frac{r_\pi}{r_b + r_\pi}}{1 + sC_t \frac{r_b r_\pi}{r_b + r_\pi}} V_{in} \quad (10)$$

ここで $r_b \ll r_\pi$ より $i_o$ は、次の式で表される。

$$V_1 \cong \frac{1}{1 + sC_t r_b} V_{in} \quad i_o = g_m V_1 \times n = \frac{g_m V_{in} n}{1 + sC_t r_b} \quad (11)$$

ここで求めた電流 $i_o$ が、図 4.39 の出力部に流れる。また、出力インピーダンスを $Z_{out}$ は以下の式のように求めることができる。

$$\begin{aligned} Z_{out} &= \frac{Z_2 \times \frac{1}{sC_p}}{Z_2 + \frac{1}{sC_p}} = \frac{Z_2}{1 + sC_p Z_2} = \frac{\frac{R_i Z_1}{R_i + Z_1}}{1 + s \frac{R_i Z_1}{R_i + Z_1} C_p} = \frac{R_i Z_1}{R_i + Z_1 + sR_i Z_1 C_p} \\ &= \frac{R_i (R_o + sL_{BW})}{(1 + sR_i C_p)(R_o + sL_{BW}) + R_i} \end{aligned} \quad (12)$$

ただし $Z_1$ 、 $Z_2$ は、以下のようになる、 $V_{OUT}$ は次式のように表すことができる。

$$Z_1 = R_o + sL_{BW} \quad Z_2 = \frac{R_i Z_1}{R_i + Z_1} \quad (13)$$

$$\begin{aligned} V_{OUT} &= Z_{out} i_o \frac{R_o}{R_o + sL_{BW}} = \frac{R_i R_o i_o}{(1 + sR_i C_p)(R_o + sL_{BW}) + R_i} \\ &= \frac{R_i R_o i_o}{R_i + R_o - \omega^2 R_i C_p L_{BW} + s(L_{BW} + R_i R_o C_p)} = \frac{\frac{R_i R_o}{R_i + R_o}}{1 - \omega^2 \frac{R_i C_p L_{BW}}{R_i + R_o} + s \frac{(L_{BW} + R_i R_o C_p)}{R_i + R_o}} \end{aligned} \quad (14)$$

今回使用する周波数領域では、 $\omega^2(R_i C_p L_{BW})/(R_i + R_o) \ll 1$ とみなせる。求めた $i_o$ を代入す

ると以下のようになる。

$$\begin{aligned}
 V_{OUT} &= \frac{\frac{R_i R_o}{R_i + R_o} g_m V_{in}^n}{\left\{ 1 + s \frac{(L_{BW} + R_i R_o C_p)}{R_i + R_o} \right\} (1 + s C_t r_b)} = \frac{R_i R_o}{R_i + R_o} g_m V_{in}^n \frac{1}{\left\{ 1 + s \frac{(L_{BW} + R_i R_o C_p)}{R_i + R_o} \right\} (1 + s C_t r_b)} \\
 &= V_{f=0} \frac{1}{\left\{ 1 + s \frac{(L_{BW} + R_i R_o C_p)}{R_i + R_o} \right\} (1 + s C_t r_b)} \quad (15)
 \end{aligned}$$

ただし、 $V_{f=0} = R_i R_o / (R_i + R_o) g_m V_{in}^n$ とする。更に $V_{OUT}$ を展開すると次式のようになる。

$$V_{OUT} = V_{f=0} \frac{1}{1 + s \left( C_t r_b + \frac{L_{BW}}{R_i + R_o} + C_p \frac{R_i R_o}{R_i + R_o} \right) + s^2 C_t r_b \left( \frac{L_{BW}}{R_i + R_o} + C_p \frac{R_i R_o}{R_i + R_o} \right)} \quad (16)$$

ここで $C_t r_b = A$ 、 $L_{BW}/(R_i + R_o) + C_p (R_i R_o)/(R_i + R_o) = B$ とすると以下のように表すことができる。

$$V_{OUT} = V_{f=0} \frac{1}{1 + s(A + B) + s^2 AB} = V_{f=0} \frac{1}{\left( s + \frac{1}{A} \right) \left( s + \frac{1}{B} \right)} = V_{f=0} \frac{1}{\left( 1 + \frac{s}{\frac{1}{A}} \right) \left( 1 + \frac{s}{\frac{1}{B}} \right)} \quad (17)$$

これは、1次のローパス特性が2段接続されたものと解釈できる。よって図4.40に示すような周波数特性になる。周波数特性が分かればA、Bから決まるカットオフ周波数のどちらが動作速度を律速しているのかが分かる。ただし、A、Bから決まる2つのカットオフ周波数は、図4.40に示すような位置関係に必ずしもなるとは限らない。なぜならA、Bの値を決める $C_t$ 、 $C_p$ は以下の式で表されカレントスイッチを構成するトランジスタの個数 $n$ 、トランジスタ1個当たりのコレクタ電流 $I_c$ および図4.41の $f_T$ - $I_c$ 特性から決まる $f_T$ の3つのパラメータによって決定する。このため回路の高速化のためには、各トランジスタに流すコレクタ電流 $I_c$ での動作点で $f_T$ が最大となるようにトランジスタサイズの最適化が必要となる。

$$C_t = \frac{qI_c}{2\pi f_T} + \frac{qI_c}{KT} \frac{R_i R_o}{R_i + R_o} n C_{jc} \quad C_p = n C_{js} + \frac{n C_{jc}}{\left( 1 + \frac{qI_c}{KT} \frac{R_i R_o}{R_i + R_o} n \right)} \quad (18)$$

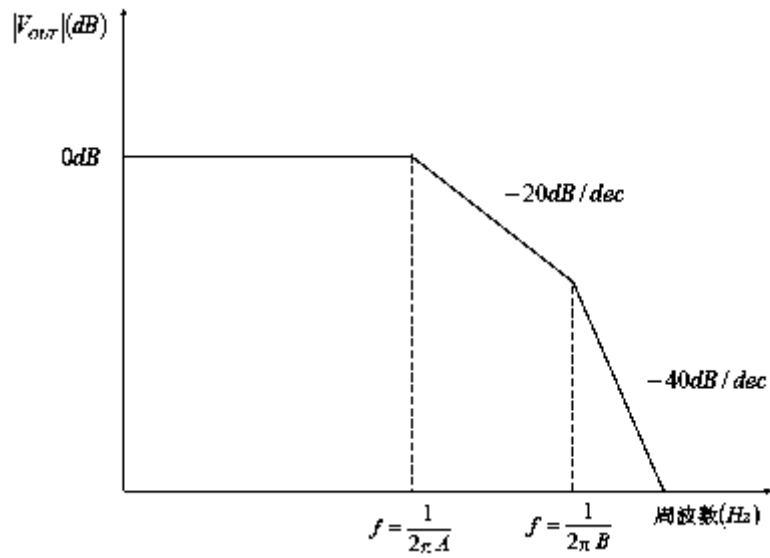


図 4.40 出力電圧の周波数特性

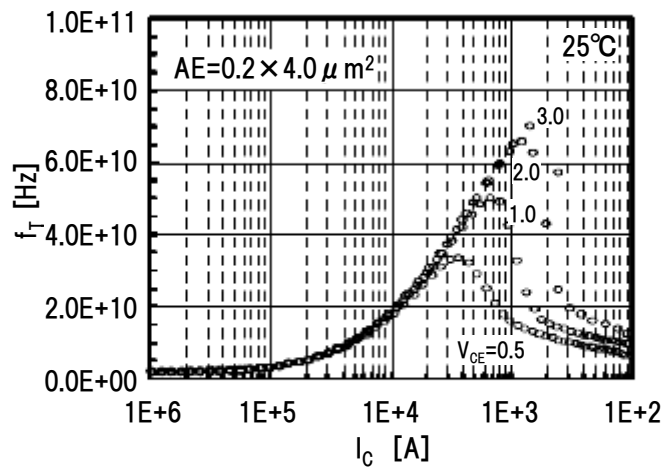


図 4.41  $f_T$ - $I_C$  特性(耐圧 3.5V)

図 4.42 のシミュレーションによる $t_r$ - $I_c$ 特性より、最も立上り時間が速いポイントは電流量 1.25mA以上の時であるが、トランジスタに流せる電流はコレクタ損失から制限されている。コレクタ損失はコレクタ・エミッタ間電圧とコレクタ電流の積で決まるトランジスタで消費される電力を示し、規定の値を超えた範囲で使用すると熱暴走により性能の低下、トランジスタの破壊を起こす。今回使用するモデルではコレクタ損失の上限値は 4.18mW である。DACの出力振幅が最大 2.5V であるためトランジスタのコレクタ・エミッタ間電圧は最大で 3.4Vにもなる。これよりコレクタ損失 4.18mWからコレクタ電流の最大値は、1.25mAとなる。よって立上り時間が最も速いポイントではなく安全な動作マージンをを考慮し、立上り時間にほとんど差のない電流量 0.8mA で使用する事に決定した。

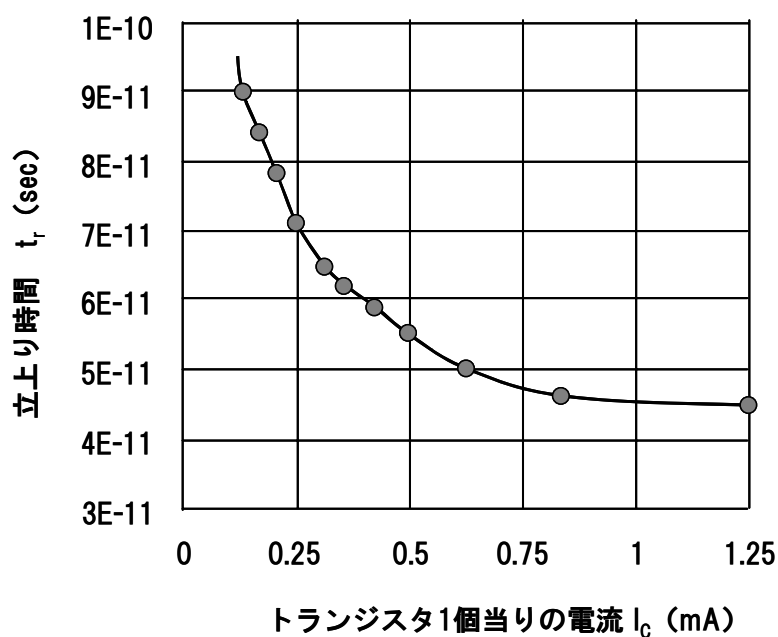


図 4.42  $t_r$ - $I_c$  特性のシミュレーション

#### 4. 7. 3 DAC IC の試作結果



図 4.43 に今回試作した 10Gbit/s、10 ビット DAC IC のレイアウト外観を示す。図左側の緑の配線はデジタル入力信号で、10 ビット差動入力であるため計 20 本の配線数となっている。入力信号間の配線長に大きな差があると配線遅延によりデータラッチ回路で正確なデータをラッチ出来なくなるため、信号間での遅延差が 0~2ps 以内に収まるように考慮し配線した。入力信号配線は GND 層とのマイクロストリップライン構造を使用している。トランジスタや抵抗などの素子の配置されていないスペースは Vcc（電源配線）と GND を前面に配置し、バイパスコンデンサを敷き詰め、電源の低インピーダンス化を図っている（入力信号配線が見えなくなるため図には表示されていない）。入力されたデジタル信号は、データラッチ回路、サーモメータデコーダとダミー回路、プリドライバ回路、カレントステアリング回路を通りアナログ信号に変換され、ワイヤボンディングの寄生インダクタンス低減のため、並列配線用の 2 つのパッドを用いて出力される。図右下の BGR（バンドギャップ基準電圧源）は、温度変化、電圧変化に対する依存性の少ない定電圧回路で構成し、IC 内部の各回路の基準電流を作る役割を果たしている。チップサイズは  $2.5 \times 2.5 \text{mm}^2$  となっている。

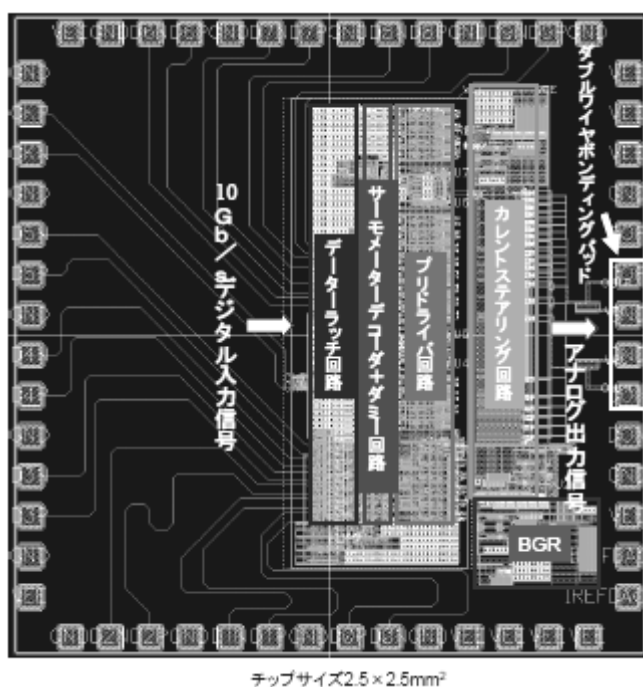


図 4.43 10Gbit/s 10 ビット DAC IC レイアウト

図 4.44 に DAC IC の測定系の構成を示す。測定条件は、測定器の環境の関係から 1 ポートのみで 10Gbit/s の信号を入力し、他の 9 ポートは直流のバイアス電圧を与えて動作を固定し、1 ポート毎に動作確認を行った。

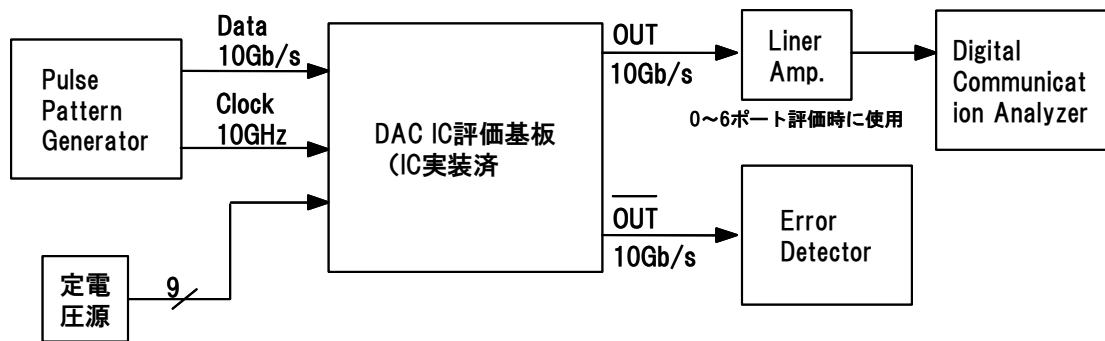


図 4.44 DAC IC の測定系

図の Liner Amp. (リニア増幅器) は、0 から 6 ポートの出力信号振幅が非常に小さいので、このポートの動作波形を観測するとき Communication Analyzer の感度能力まで信号振幅を増幅している。

図 4.45 に観測した各ポートの出力波形を示す。

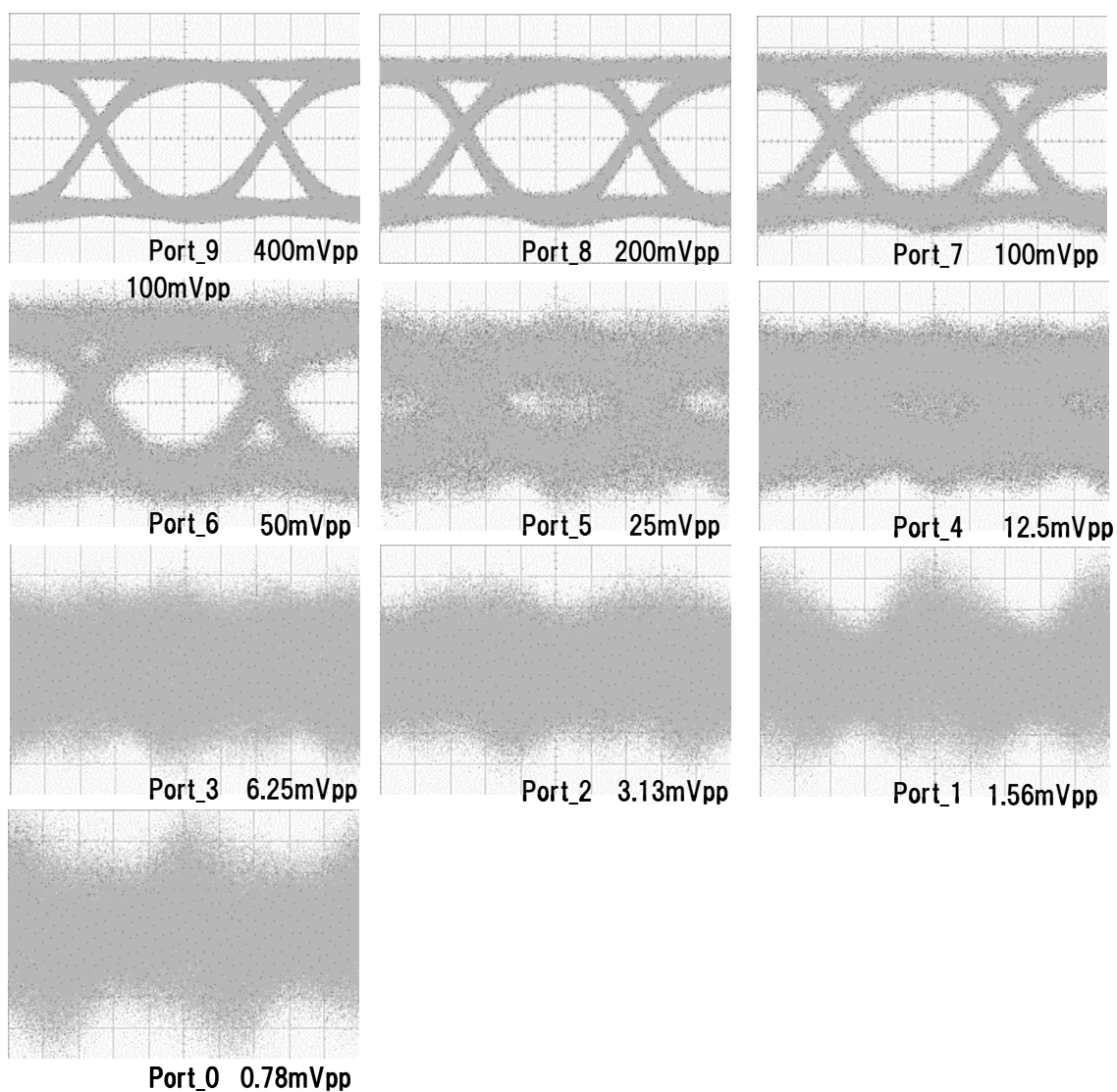
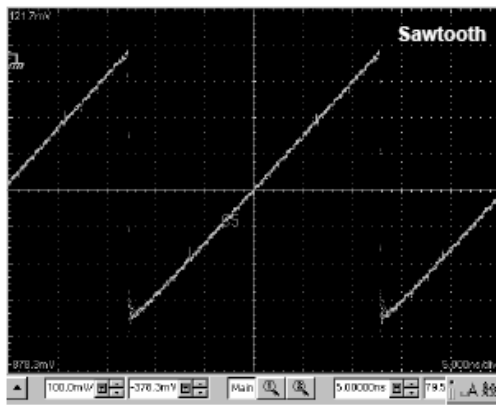


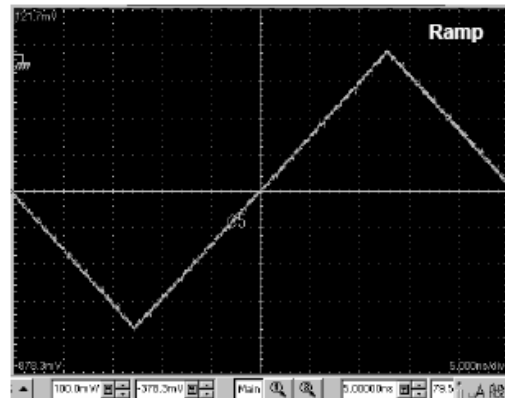
図 4.45 観測した各ポートの出力波形

ポート 6 までは、10Gbit/s 動作を確認することができるが、5 ポート以下のポートでは使用しているリニア増幅器と測定器（Communicatio Analyzer）および測定系の雑音の影響や精度で正確な波形観測は不可能であるが波形の変化と振幅の推移は確認できた。

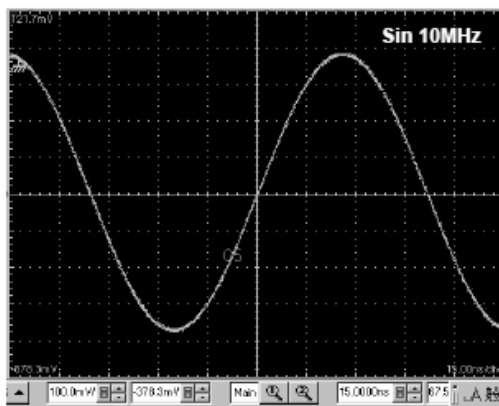
更に DAC の基本動作である波形生成機能を確認するため、のこぎり波、ランプ波、正弦波のテストパタンデータを入力し、これらに対して波形生成精度の確認がしやすい周波数の低い条件で測定を行い、図 4.46 に示すような良好な動作波形を確認することができた。



(a) のこぎり波 (100mV/div., 5ns/div.)



(b) ランプ波 (100mV/div., 5ns/div.)



(c) 正弦波 (100mV/div., 15ns/div.)

図 4.46 テストパターン出力波形

図 4.47 に試作した 10Gbit/s Y-00 暗号化光送受信機の外観を示す。送信機、受信機ともに 19 インチの 2 ユニット幅 (高さ) の標準ラックサイズに納まっている。また、図 4.48 に受信機の装置内部を示す。吹き出しで示した部分の金属ブロックで囲まれたセラミック基板上に DAC IC が実装されている。尚、送信機も基本的に同様な実装配置になっている。



(a) 10Gb/s Y-00 送信機

(a) 10Gb/s Y-00 受信機

図 4.47 試作した 10Gbit/s Y-00 暗号化光送信機、受信機

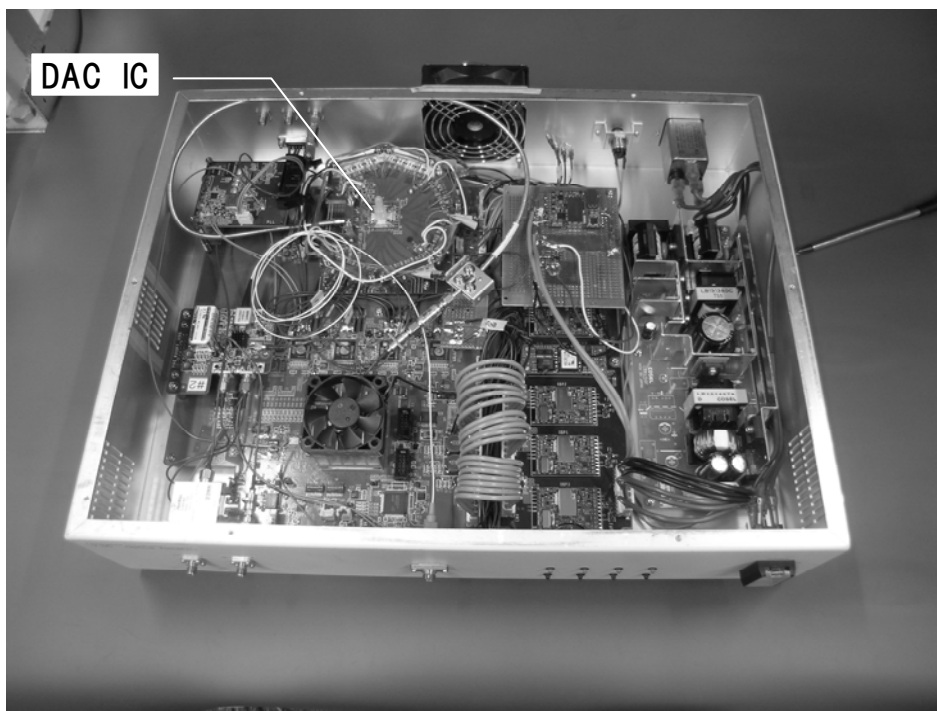


図 4.48 試作した 10Gbit/s Y-00 暗号化光受信機内部

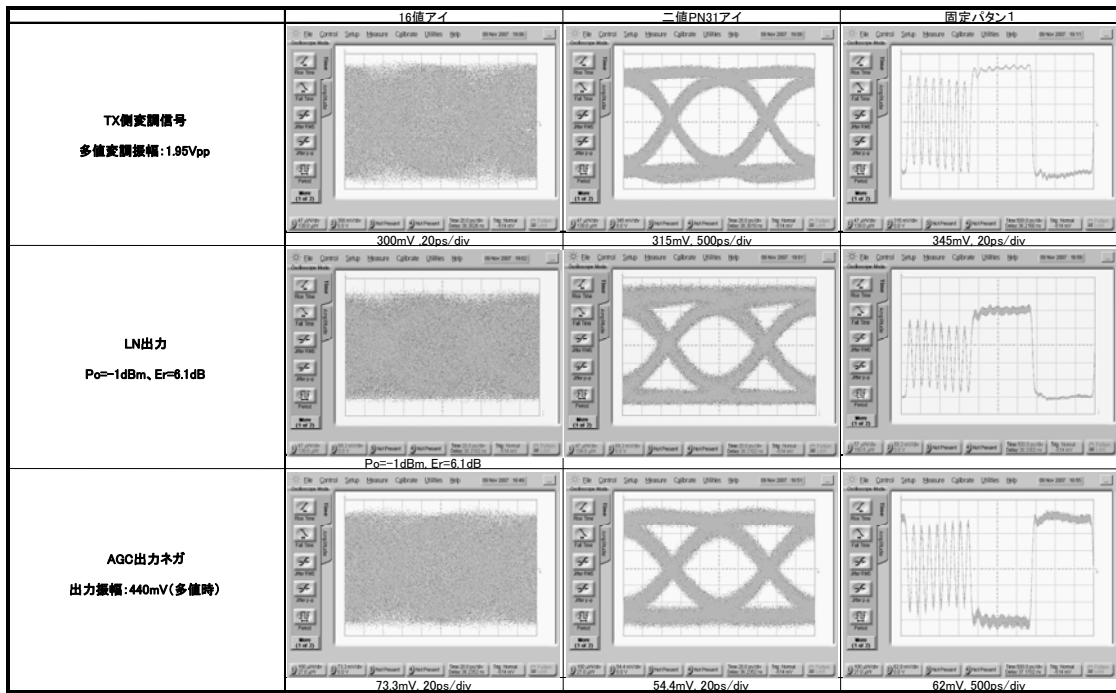


図 4.49 10Gbit/s Y-00 暗号化光送信機、受信機の各部の波形

図 4.49 に試作した Y-00 暗号化光送信機、受信機の各部の波形を示す。上段は、送信機の変調波形 (TX 側変調波形)、中段は LN 外部変調器で変調を行った送信機の光出力 (LN 出力) 波形であり、下段は受信機で信号を受信した後の等価増幅波形であり、AGC 増幅器出力のネガ側 (AGC 出力ネガ) の波形である。各波形は、図の左から 16 値、2 値の PN31 段のアイパターン波形、固定パターンである。表 4.4 に主要特性を示す。

表 4.4 10Gbit/s Y-00 暗号化送受信機の主要特性

NO.	項目	単位	性能
1	ビットレート	Gbit/s	9.95328
2	光出力パワー	dBm	-1
3	光出力波長	nm	1550
4	光消光比	dB	6.1
5	暗号化多値数	値	16
6	正規送受信受信感度	dBm	-9

また、正規受信者と盗聴者を想定した受信感度の比較のエラーレート特性を図 4.50 に示す。正規受信者は、多値数 16 値、受信感度が-9dBm において何とか誤り率 (BER) が  $1E-12$  を満足しているが、誤り率特性はフローアをはいており、 $1E-8$  付近から急激に曲がりだしている。この現象は、装置内の主信号系回路全体での総合帯域の不足、特に受信機の受信信号を変動閾値 (10Gbit/s の変動閾値動作) を用いて暗号の複合を行っている部分の影響が大きく、受信波形のジッタが大きくなることが劣化要因として判明している。

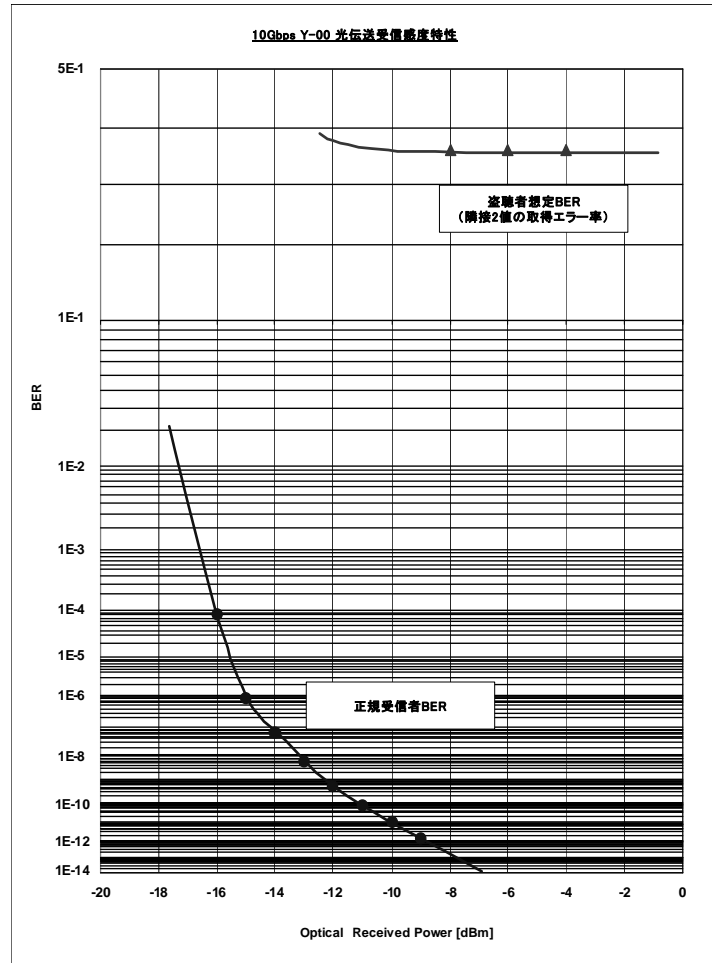


図 4.50 正規受信者と盗聴者を想定した受信感度の比較

#### 4. 8 まとめ

光強度変調型光通信量子暗号 Y-00 方式を適用した光送受信機を試作し、商用回線を用いた 3 中継伝送実験により Y-00 方式の有用性を実証した光送受信機は伝送速度が STM16 および OC-48 に準拠した 2.5Gbit/s であり、50km の無中継伝送が可能である。伝送実験では、3 台の光ファイバ増幅器を中間中継器として使い、総延長 196k の商用回線においてエラーフリーであることを確認した。また、商用回線を用いた WDM 伝送実験により、既存の標準通信プロトコルとの親和性も確認でき、早期実用化への見通しを得ることができた。



更に、Y-00 方式が既存の公衆通信基幹ネットワークのみならず、イーサネットやファイバチャネルネット等を包含する次世代ネットワークへの適応も可能なことを明らかにできた。本システムはアメリカ等で実験されている基本 Y-00 より安全性が高いが、まだ厳密な安全性の定量化は測定装置の精度が理想的にはならないため難しい。

また、更に高速化を目指し、10Gbit/s (OC-192/STM32) 伝送に対応させるため、Y-00 暗号化を専用に行う高速な 10 ビット DAC を開発し、これを搭載した 10Gbit/s Y-00 暗号化送受信機の試作を行った。この試作機で 10Gbit/s の基本動作確認を行い、安定した安全性を確保するための幾つかの問題点を抽出することができ、10Gbit/s 伝送システムへの適応性について見通しを得ることができた。今後の課題として、高精度な安全性評価装置を開発して厳密な評価を実施する。。

## 第5章 結論

将来の光通信システムに要求される課題について光送受信機を中心に研究を進め、装置の高精度化の特性と低価格化の両立を実現する光送受信機の自律制御アーキテクチャを提案し試作結果を基に、そのアーキテクチャの有効性を検証した。また情報ネットワークの物理的な安全性を確保する要求に対して、量子情報通信分野においても早期実現性に期待がもたれている量子暗号を取り上げ、その中でも既存の光通信ネットワークとの親和性が高いと思われる Yuen2000 プロトコル理論を応用し、既存システムである光強度変調への適用を考え、光通信量子暗号 (Y-00) 伝送装置の開発を行った。その試作結果から伝送路の物理的に高度な安全性を確保すると共に、既存の光通信プロトコルや伝送システムとの親和性について検証実験を行い早期実用化への見通しを得ることができた。

## 謝辞

本研究に関しましては多くの方々からの御指導、御協力を頂きました。

鹿児島大学工学部、山下喜市教授には、本研究および本論文をまとめるにあたり日々に渡り多大なる御指導を戴きましたことを深く感謝いたします。また予備審査委員として本論文の纏め方を中心に、御指導を戴きました同大学の高田等教授に深く感謝いたします。本研究を進める上で IC および LSI 開発におきまして多大なる御指導と御協力を戴き、また本論文を纏める上で御指導を戴いた大畠賢一准教授にも深く感謝いたします。更に光通信量子暗号 (Y-00) の研究においては、理論の御教授と研究の企画・遂行にあたり多大なる御指導および御支援を戴いた玉川大学学術研究所の広田修教授に深く感謝いたします。

本研究は、複数の国家プロジェクトのも関連しており、多くの方々に御協力を戴いております。WDM 光伝送装置用アーキテクチャの研究においては、平成 16 年度、17 年度地域新生コンソーシアム研究開発事業における「光 WDM 伝送用自律制御アーキテクチャとシステム L S I の開発」の共同研究において LSI の実装で多大な御協力を戴いた (株) 日本計器鹿児島製作所の浮辺淳一工場長、加藤正明部長、池崎勉さん。MPU 開発で多大なる御協力を戴いた慶應義塾大学理工学部、西宏章准教授および鹿児島大学山下・大畠研究室卒業生で LSI の設計で御協力戴いた小野宏一さん、田口量寛さん、犬塚正道さん、上村勇仁さん。アーキテクチャの制御シミュレーションの検討戴いた寿村理恵さんをはじめ関係者の方々に感謝いたします。更に鹿児島大学山下・大畠研究室在校生で光通信量子暗号伝送装置用 IC の開発で御協力戴いている清水雅裕さん、宇野哲史さん、迫紘平さん、今村裕典さんおよび関係者の方々に感謝いたします。

また日立情報通信エンジニアリング株式会社で研究の機会を与えて与えてくださいました若井勝郎取締役社長、並びに坂口貢取締役をはじめ御指導戴いた幹部および上長の方々に深く感謝いたします。更に本研究において日々一緒に開発を進めて戴いた、本田真さん、平塚和也さん、池邊寛さん、池内英洋さん、坪重人さんをはじめ関係者の皆様に深く感謝いたします。

本研究をまとめることができたのは、上記の方々の御指導、御支援、御協力の賜物であり本論文を結ぶにあたり心からの誠意を表わすしだいです。

そして最後に、これまで支えてくれた両親および家族に感謝いたします。

## 参 考 文 献

- [1] AKARIプロジェクト著, “新世代ネットワークアーキテクチャAKARI概念設計書”, 総務省, 2007年4月
- [2] A.H. Gnauck, G. Chalet, P. Tran, P. Winzer, C.R. Doerr, J.C. Centanni, E.C. Burrows, T. Kawanishi, T. Sakamoto and K. Higuma “25.6-Tb/s C+L-Band Transmission of Polarization-Multiplexed RZ-DQPSK Signals”, OFC2007, PDP19, Anaheim, USA, 29 March, 2007
- [3] H. Takara et al., “Field demonstration of over 1000-channel DWDM transmission with supercontinuum multi-carrier source,” Electron. Lett. Vol. 41, pp.270 (2005)
- [4] Y. Miyagawa et al., “Over-10 000-channel 2.5 GHz-spaced ultra-dense WDM light source,” Electron. Lett. Vol. 42, p.655 (2006)
- [5] B.Villeneuve, M.Cyr, H.B.Kim, ”High-stability wavelength-controlled DFB laser sources for dense WDM application”, OFC’98, 381, 1998.
- [6] K.Tatsuno, M.Shirai, H.Furuichi, K.Kuroguchi, N.Baba, H.Kuwano, Y.Iwafuji, A.Murata, ”50GHz spacing, multi-wavelength tunable locker integrated in a transmitter module with a monolithic-modulator and a DFB-laser”, OFC’2001, 1, 2001.
- [7] H.Nusu, T.Mukaihara, T.Nomura, A.Kasukawa, M.Oike, T.Shiba, Ninomiya, ”25 GHz-spacing wavelength monitor integrated DFB laser module using standard 14-pin butterfly package”, OFC’2002 , 209,2002.
- [8] 坂井猛, 小栗均, 時田宏典, ” 温度高安定性波長ロッカーの開発”, (株) 応用光電, TECHNICAL REPORT, 1,2002.
- [9] 山原建二, 原澤克嘉, 塙洋明, 羽田誠, ” マイコン制御 STM-4 対応光送信器の開発”, 1997 年度電子情報通信学会総合大会, B-10-123 , 1997.
- [10] 前田 靖, 他 10 名, ” DWDM 対応 SFP 型光トランシーバーの開発” , SEI テクニカルレビュー第 168 号, 2006.
- [11] 米田晴紀, 他 7 名, ” 2.5Gbps 超小型波長可変光送信モジュールの開発” , SEI テクニカルレビュー第 161 号, 2002..
- [12] ITU-T Recommendation, G692
- [13] A.S.Holevo, M.Sohma, and O.Hirota, ” Capacity of quantum Gaussian channels” ,

Physical Review A, vol.59, no.3, pp.1820-1828, 1999

[14] E.Corndorf, C.Liang, G.S.Kanter, P.Kumar, and H.P.Yuen, "Quantum noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks", Physical Review A, vol. 71, 062326, 2005.

[15] R.Nair, H.Yuen, E.Corndorf, T.Eguchi, and P.Kumar, "Quantum noise randomized ciphers", Physical Review , A 74, 052309, 2006

[16] 広田 修, 山下喜市, 原澤克嘉, 布施 優, 大畠賢一, "光通信量子暗号 Y-00 の安全性能力評価装置", 電子情報通信学会, 光通信システム研究会, 2007 年 6 月 14 日

[17] O.Hirota, K.Kato, M.Sohma, T.Usuda, and K.Harasawa, "Quantum stream cipher based on optical communications", Proc. on quantum communication and imaging II, SPIE, vol-5551, 2004.

[18] O.Hirota, K.Kato, M.Sohma, and M.Fuse, "A quantum symmetric key cipher (Y-00) and key generation: Quantum stream cipher part II", Proc. on quantum informatics, SPIE, vol-5833, 2004

[19] Katsuyoshi Harasawa, Makoto Honda, Seiichi Iwata, Nobuaki Kanazawa, Tomohiro Kanamaru, Osamu Hirota, "Basic experiment of quantum cryptography based on optical communications", 2004 年電子情報通信学会通信ソサイエティ大会, B-10-34, 2004 年 9 月.

[20] 細井, 原澤, 本田, 坏, 小林, 広田, "2.5Gb/s 光通信量子暗号 Y-00 伝送装置のフィールド伝送実験", 電子情報通信学会総合大会, B-10-80, 2007 年 3 月.

[21] Fuse, M. Furusawa, S. Ikushima, T. Hirota, O., "Development of an ultra high-secure and 1Gb/s optical transmission system using quantum noise diffusion cryptography", ECOC 2005. 31st European Conference on Optical Communication

[22] 原澤 克嘉, 広田 修, 山下 喜市, 本田 真, 坏 重人, 細井 健司, 土井 吉文, 大畠 賢一, 片山 武彦, 清水 哲也, "Yuen 2000 プロトコルによる物理暗号のための Randomization の実装回路の考察", 電子情報通信学会 論文誌 B 投稿中

[23] C.W.Helstrom, "Quantum detection and estimation theory", Academic Press, 1976

[24] 広田 修, "光通信理論", 森北出版, 1985

[25] M.Osaki, M.Ban, and O.Hirota, "Derivation of the optimum detection operator and

its physical interpretation for coherent state signals”, *Physical Review A*, vol.54, no.2, pp.1691-1701, 1996.

[26] 広田, ” 光通信ネットワークと量子暗号” , 論文誌 B, No-4, pp 478-486, 2004.

[27] Osamu Hirota, ”Practical security analysis of a stream cipher by the Yuen 2000 protocol” , *PHYSICAL REVIEW A* 76, 032307 (2007).

[28] Osamu Hirota , Tetsuya Shimizu, Takehiko Katayama, Katsuyoshi Harasawa, ”10 Gbps quantum stream cipher by Y-00 for super HDTV transmission with provable security”, *Proc. of SPIE*, Volume 6710, *Quantum Communications and Quantum Imaging V*, Ronald E. Meyers, Yanhua Shih, Keith S. Deacon, Editors, 67100K (Sep. 25, 2007).

[29] 坏重人, 土井吉文, 細井健司, 本田真, 原澤克嘉, 広田修, 片山武彦, ” 光通信量子暗号 (Y-00) 伝送装置のフィールド多段中継伝送実験” , 2007 年電子情報通信学会ソサイエティ大会, B-10-29, 2007 年 9 月.

[30] Osamu Hirota, Masaki Sohma, Masaru Fuse, and Kentaro Kato, ”Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme.”, *Physical Review A* -72, 022335, 2005

[31] 小林洋平, 水上勇輝, 渡部圭, 広田修, ” 光通信量子暗号 (Y-00) における量子ゆらぎエラーの均一化” , 2006 年電子情報通信学会総合大会, B-10-38, 2006 年 3 月

[32] 清水哲也, 広田修, ” 光通信量子暗号 Y-00 ランニング鍵ランダム化” , 電子情報通信学会, 技報 OCS,PN,CS 研究会, 2007 年 6 月 14 日.

[33] S.Donnet, A.Thangaraj, M.Bloch, J.Cussey, J.Merolla, ”Security of Y-00 under heterodyne measurement and fast correlation attack”, *Physics Letters A*, 356, pp406-410, 2006.

[34] 原澤克嘉, 広田修, 山下喜市, 本田真, 坏重人, 細井健司, 土井吉文, 大畠賢一, 片山武彦, 清水哲也, ”Yuen 2000 プロトコルによる物理暗号のための Randomization の実装”, 電子情報通信学会, 和文論文誌 C, (2008 年採録決定) .