



超多重RFIDシステムの設計手法

福水, 洋平

(Degree)

博士 (工学)

(Date of Degree)

2007-03-25

(Date of Publication)

2009-09-11

(Resource Type)

doctoral thesis

(Report Number)

甲4004

(URL)

<https://hdl.handle.net/20.500.14094/D1004004>

※ 当コンテンツは神戸大学の学術成果です。無断複製・不正使用等を禁じます。著作権法で認められている範囲内で、適切にご利用ください。



博 士 論 文

超多重RFIDシステムの設計手法

平成19年2月

神戸大学大学院自然科学研究科

福 水 洋 平

要旨

本研究は RFID¹システムの高多重化に関するものである。ユビキタス社会の到来に伴って、「いつでも」「どこでも」コンピュータ・ネットワークにアクセスできるような基盤が整いつつある。このような流れの中で、RFID 技術はユビキタスの根幹を担う個体識別のための重要な技術として世界的に注目を浴びている。個体識別システムは「そこに何かがあるか」を自動的に認識し、業務効率を改善するために用いられる。たとえば、商品の入荷や在庫の管理で今日幅広く用いられている個体識別システムとしてバーコードがある。ところが、バーコードは光学走査によって実現されるため、シンボルの汚損に弱いだけでなく、個々に識別処理を行う必要があり識別効率が低い。

これらの問題を解決する技術として RFID が位置づけられている。RFID は非接触かつ自動で高速に物品を識別できることから次世代の個体識別システムとして応用する動きが活性化している。たとえば、流通では生産拠点で商品に RFID タグを貼り付ける。タグは一意の ID を持っていて、貼り付けた段階で「何に」「どの ID の」タグを貼り付けたかをデータベースに登録する。商品は物流拠点を通るたびに照合され、ロストしていないかを確認められる。最終的に小売店に到達し、入荷処理や在庫管理、販売時の会計処理に用いられる。このような応用を考えると、大量の商品を取り扱う必要があるため、個々の商品の識別にかかる時間を短縮する必要がある。

RFID はバーコードのように個々に識別させる場合でも十分に認識効率が高いが、一括して RFID タグを識別することを可能とする技術の開発が必要である。そのためには、RFID を構成するトランスポンダとリーダーの間における識別情報の交換を効率よく多重化する必要がある、数多くの衝突防止アルゴリズムが研究、開発されてきた。RFID において複数トランスポンダと単一リーダー間の衝突防止技術は決定的手法と確率的手法に分類される。

個々のトランスポンダに対してリーダーが個別に ID 情報を問い合わせる決定的手法として、Query Tree や Binary Search をはじめとする様々な

¹Radio Frequency Identification

手法が研究されている。このアルゴリズムは箱の中身を出すことなく物品の識別が可能ではあるが、達成できる識別速度に限界があった。一方、FTDMA をはじめとする確率的手法に基づく衝突防止アルゴリズムは非常に高い効率でトランスポンダを識別することができる。これは、トランスポンダにランダムで多重通信チャネルを割り当てさせ、自発的にID情報を送信させることによって、リーダが個々に問い合わせなくても大量のタグ識別を達成することができる。現在、実用化されているRFIDの確率的衝突防止アルゴリズムで最速のものが1秒に600個程度である。

本研究は流通への応用を想定して、この最速のものを遥かに凌駕する400ミリ秒に1,000個の識別を達成するRFIDシステムの開発を目標とする。この目標を達するため、本研究ではTS-CDMA²通信に基づいた衝突防止アルゴリズムを考案した。確率的手法はトランスポンダが自発的にチャネル選択を行うため、衝突率をゼロにすることはできない。そのため提案したアルゴリズムは、

- (1) トランスポンダからリーダへの応答を TS-CDMA 方式により多重化して送信
- (2) ランダムプロセスによるチャネル選択で複数の応答が衝突した場合は CRC を用いて誤り検出
- (3) ノイズや衝突により生じた誤りは破棄
- (4) 通信誤りに対しては再送により回復

以上4つのアイデアから構成されている。ここで、物流向けRFIDはユーザビリティのため電池を内蔵することができない。すなわち、トランスポンダはリーダから誘導結合により電力を供給されなければならないので、その消費電力および回路規模を可能な限り削減しなければならない。そこで、提案アルゴリズムは衝突や誤りが発生したかどうかに関わらず、トランスポンダがランダム選択と再送を繰り返すことで、処理が複雑にならないように配慮している。その上で、本アルゴリズムを用いて目標の識別速度を達成する、RFID向けの通信方式を提案した。数理的な分析に基づき、その誤り率は $2.52e-9$ と求められた。

続いて、通信方式を実現する回路方式を提案した。トランスポンダを簡素にするため、TS-CDMA で必要となる送受信間の同期はリーダが輻射する電力波を180度、位相シフトすることによって行われる。この同期

²Time Slotting-Code Division Multiple Access

パルスを検出する回路を SRFF³と DFF⁴で簡素に実現した。また、設計した回路方式と一次変復調は回路レベルシミュレーションと試作チップを使った実験で確かめることができた。

この提案方式を実証するためには 1,000 多重通信の検証が必要である。しかしながら、1,000 個のトランスポンダから成る多重通信を回路シミュレータやチップ試作で実現することは、演算規模や試作コストを考慮すると困難である。そこで多重通信を評価するために高位モデル化による評価システムを構築し、デジタルバックエンドの設計手法を提案した。評価システムは 2 種類の高位モデルから構成されている。

- (1) FPGA⁵を用いたハードウェア・エミュレータ
- (2) カスタムソフトウェア・シミュレータ

である。

エミュレータは 2 枚の FPGA ボードを用いて実現した。1,000 個のトランスポンダを再現するボードと、リーダ用のボードから成り立っている。FPGA はアナログ信号を扱えないので、この 2 枚のボードはデジタルで直結されている。また、外乱として白色ノイズをデジタル表現でモデル化し組み込むことで、ノイズに対するデジタル処理のロバスト性を評価することが可能とした。このエミュレータは、ハードウェアの並列性により多重通信における衝突率を求めるための確率試行を高速に実施することができる。エミュレータによる検証を通して以下の RFID システム設計の際に重要な点を見い出した。

- (1) 再送数の誤り率に対する影響は大きい。
- (2) ノイズを考慮すると、リーダの相関器における閾値の誤り率に対する影響は大きい。
- (3) 一方で閾値を低下させると存在しない ID が生じる確率が高まる。

次に、RFID システムの設計にあたって無視することができない外乱による性能への影響を評価するためにシミュレータの開発を行った。エミュレータと異なり、ソフトウェアで実装されているため外乱の影響に対するロバスト性の評価をエミュレータより柔軟に行うことが可能となった。また、システムパラメータについても柔軟に設定することができ、機能

³Set Reset Flip-flop

⁴Data Flip-flop

⁵Field-Programmable Gate Array

拡張も極めて容易である。シミュレーションの結果はリアルタイムに視覚化することで、応答の衝突や伝送誤りの傾向を容易につかむことが可能である。提案シミュレータによる検証を通して、RFID システムの設計に重要な以下の結論を得た。

- (1) チャンネルノイズの影響を想定しても再送数は誤り率に対して影響が大きい。
- (2) 識別領域に存在するトランスポンダが 1,000 を超過する場合も再送数が重要な影響を与える。
- (3) TS-CDMA における TDMA⁶と CDMA の配分はノイズ耐性に影響をおよぼす。

これらの高位モデルによる評価システムを用いた分析を通して多重通信パラメータとデジタルバックエンド設計を最適化した。これにより、高位モデル化手法に基づく 1,000 チャンネルの RFID システムのバックエンド設計手法を確立した。

以上の通信手法および設計手法により RFID システムのデジタルによる多重通信において提案アルゴリズムの有効性が確かめられたものの、RFID は一次変調や電磁結合に代表されるアナログ領域も含んでいるため、より現実に近いシミュレーションを行ってシステムの動作性能を検証する必要がある。特に 1,000 多重 RFID は試作が容易ではないため、設計と並列してモデル化でき、設計結果をバックアノテーションにより検証してシステム設計にフィードバックできるような評価システムが望まれる。そこで、提案したバックエンド設計のためのソフトウェアシミュレータを改良し、これを Verilog-AMS シミュレータと統合した。このシミュレーション環境は RFID システムの設計においてなくてはならないツールである。

アナデジ混載のシミュレーションを実現すると同時にシステムパラメータや通信方式の柔軟な設定変更を可能とするために、構築した統合シミュレーション環境は Verilog の PLI⁷機能を用いてソフトウェアと Verilog-AMS シミュレータを接続する。Verilog-AMS は SPICE モデルを組み込むため、ハードウェア設計やチップ設計と並列して評価システムの具体モデル化が可能である。すなわち、これらの設計結果をモデルに組み込むことができる。抽象度を自由に選べるので、より多くの外乱に対し

⁶Time Division Multiple Access

⁷Program Language Interface (プログラム言語インタフェース)

てロバスト性評価ができるようになった。このシミュレーション環境によって、

- (1) 誤り率の再送への効果
- (2) ノイズによって一次変調がもたらす通信誤りの影響
- (3) 相関器の閾値によるノイズ耐性への影響が確かめられた。

アナログ信号処理モデルを含んでいるため、より現実に即したシミュレーションが可能となった。これにより、RFID システム全体の評価ができるようになり、超多重 RFID のシステム設計手法を確立した。

半導体の微細化に伴う SoC⁸技術の発展によって、今後ますます半導体設計におけるシステムレベル設計が重要視される時代が到来した。本研究で明らかにしたトップダウン・アプローチによる設計手法は、このようなアナデジ／ミックスドシグナルの SoC 開発において特に有効である。

⁸Systems-on-a-Chip

目次

1	緒論	1
1.1	研究の主旨	1
1.2	個体識別システム	2
1.2.1	バーコード	2
1.2.2	光学文字認識	5
1.2.3	生体認証	5
1.2.4	磁気カード	5
1.2.5	IC カード	6
1.2.6	RFID	6
1.3	RFID における衝突問題	9
1.3.1	複数のリーダが近傍に存在することによる衝突	9
1.3.2	複数のトランスポンダとリーダの衝突	15
1.4	従来研究	15
1.4.1	決定的手法による衝突防止	16
1.4.2	確率的手法による衝突防止	30
1.4.3	本研究の位置づけ	33
1.5	研究の概要と本論文の構成	35
1.5.1	超多重 RFID システムの通信方式の提案	35
1.5.2	高位モデル化によるバックエンド設計手法の提案	36
1.5.3	統合シミュレーション環境によるアナデジ混載チップの設計手法の提案	36
2	超多重 RFID システムの通信方式の提案	37
2.1	緒言	37
2.2	システムアーキテクチャ	38
2.2.1	想定する応用例	38
2.2.2	システムパラメータ	39
2.2.3	電磁パラメータ	40
2.3	超多重 RFID 向け通信方式	42
2.3.1	概要	42

2.3.2	ダウンリンク	44
2.3.3	アップリンク	45
2.3.4	通信制御	49
2.3.5	誤り検出	52
2.3.6	通信時間	54
2.4	超多重 RFID の回路方式	54
2.4.1	トランスポンダの構成	54
2.4.2	リーダの構成	61
2.5	回路方式の設計検証	63
2.5.1	回路レベルシミュレーションによる検証	63
2.5.2	プロトタイプ実装	63
2.5.3	実験による基礎検証	66
2.6	結言	68
3	高位モデル化によるバックエンド設計手法の提案	71
3.1	緒言	71
3.2	ハードウェア・エミュレータによるビヘイビアモデル	72
3.2.1	ノイズによる応答信号の減衰	72
3.2.2	アーキテクチャ	74
3.2.3	リーダ・ユニットの構成	74
3.2.4	トランスポンダ・ユニットの構成	76
3.2.5	疑似チャネルの実現	77
3.2.6	TDMA チャネルと再送数の関係	78
3.2.7	閾値によるノイズへのロバスト性	80
3.3	ソフトウェア・シミュレータによる高位モデル	82
3.3.1	シミュレータの概要	82
3.3.2	シミュレーションシステムの動作フロー	86
3.3.3	1,000 を超える RFID 多重通信の解析と設計	86
3.3.4	RFID 通信における外乱の影響	88
3.3.5	ロバストな RFID 通信向けバックエンドの設計	92
3.4	結言	94
4	統合シミュレーション環境によるアナデジ混載チップの設計手法の提案	95
4.1	緒言	95
4.2	統合シミュレーション環境	96

4.2.1 システムの概要	96
4.2.2 AFE モジュールの回路レベル記述	98
4.2.3 DBE モジュールのシステムレベル記述	99
4.2.4 動作シーケンス	100
4.2.5 ISE の実装に伴う課題	101
4.2.6 ISE 援用によるチップ設計	103
4.2.7 他の従来モデルとの比較	105
4.3 1,000 を超える RFID システムのプロトタイプ	108
4.3.1 チャネルノイズの影響	108
4.3.2 信号電力の変動による影響	109
4.4 結言	112
5 結論	115
謝辞	123
参考文献	125
発表論文一覧	137
本研究に関する発表論文	137
学術雑誌	137
国際会議	137
学術講演	138
口頭発表	138
図一覧	139
表一覧	143
A 通信の多重化	145
A.1 概要	145
A.2 FDMA	145
A.3 TDMA	146
A.4 OFDM	146
A.5 SDMA	147
A.6 CDMA	147
略語一覧	149

第1章

緒論

1.1 研究の主旨

本研究は Radio-Frequency Identification (RFID) システムの高速多重化に関するものである。ユビキタス社会の到来に伴って、「いつでも」「どこでも」コンピュータ・ネットワークにアクセスできるような基盤が整いつつある [1-3]。このような流れの中で、RFID 技術はユビキタスの根幹を担う重要な技術として世界的に注目を浴びている。RFID システムの起こりは第2次世界大戦の航空戦闘における敵と味方の自動識別 [4] にあるといわれている。すなわち、敵の戦闘機だけを効率よく撃墜するために、味方の航空機にトランスポンダといわれる自動応答装置を装備させ、応答しないものに対してのみ攻撃を加える対空砲や戦闘装備を配備することによって、航空戦力の無効化を目指したものである。この自動応答による航空機識別の仕組みは 1960 年代に民用化され、今日では航空機の自動認識から大きく発展を遂げた [5]。さまざまな物品や個人を識別するシステムとして流通や在庫の管理のみならず、電子マネーの実現や鉄道の改札における非接触化、あるいは有価証券の偽造防止など幅広く活用され始めている [6, 7]。RFID に関連して、近年ではセンサーネットワークと呼ばれる技術も大きく注目されている [8, 9]。これは能動的に動作するセンサーノードが自発的にセンシング結果を応答することによって、現実世界の状態をコンピュータネットワークに反映させる技術なのでユビキタス社会において重要な位置を占める技術であるといえる。センサーネットワークも RFID から派生した技術であり、その根幹である RFID の重要性は増える一方である。このように、将来的に必要不可欠な技術となりつつある RFID であるが、市場における運用に関してはいまだ実験段階にとどまっている。本研究では、これまで研究されてこなかった RFID システムの高速読み取りに焦点を絞って、新たに通信方式から提案を行うものである。

1.2 個体識別システム

個体識別システムは「そこに何かがあるか」を自動的に認識し、この情報をコンピュータで処理することにより業務効率を改善するために用いられる。たとえば、商品の入荷や在庫の管理で今日では幅広く用いられている Point-of-Sale (POS) システムでは、入荷した商品や売れた商品を個体識別システムの一つであるバーコードで自動かつリアルタイムに認識する。商品価格が自動的に求められるので、会計処理が大幅に省力化されるだけでなく、在庫残数や本日の売り上げなどの情報処理により戦略的な販売活動を可能とする。このように現実社会とコンピュータをつなぐ基盤となる個体識別技術は、情報技術の発展とともに今や様々な分野の業態で必要とされている。この技術により実現されるシステムを個体識別システムと呼び、本節では代表例として、バーコード・光学文字認識・生体認証・磁気カード・IC¹カード・RFID の各々について解説を行う。

1.2.1 バーコード

市場に流通するほとんどの商品や物品に貼付されるバーコードは、過去 40 年間にわたって物品や商品を自動管理するために用いられてきた。その応用範囲は幅広く、販売・流通のみならず製造やサービスなどあらゆる場面で目にすることができる情報媒体である。そのため、今日では世界各国で毎日 50 億個のバーコードが利用されており [10, 11] 非常に大きな市場を構成している。

バーコードは平行に並べられた黒線の太さとその間隔によって情報をバイナリ表現する。その縞模様状のパターンはレーザーや発光ダイオード (Light-Emission Diode; LED) を使った光学的走査、すなわち黒線と間隔部分の異なる光の反射率を利用して、パターンに直接強い光を当てて読み取り、それによってコードが表現する情報を得ることができる。黒線と間隔によって情報表現するという本質的な部分以外に、どんな情報をどれだけの大きさにコード化するかという点で種々の規格があり、代表的なものに UPC、JAN/EAN、ITF、CODE-128、CODE-39、NW-7 があげられる。各バーコードの例を Figure 1.1 に図示する。

このようにバーコードは印刷によって識別情報を物品に付与できるため、個々の認識対象にかかるコストを非常に低く抑えることができる。一

¹Integrated Circuit

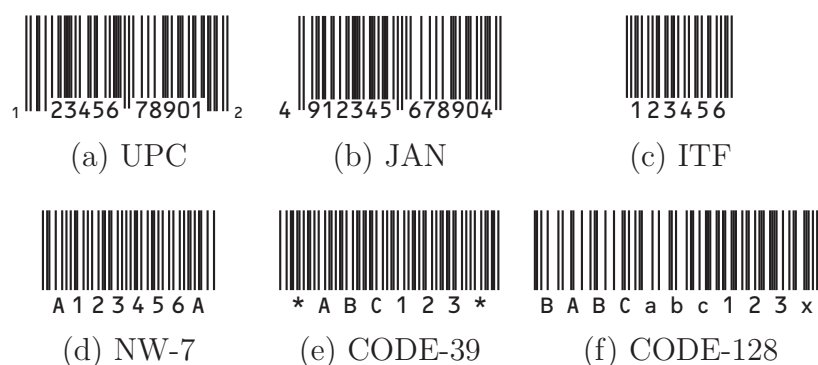


Figure 1.1: 各標準規格に基づくバーコードのパターン例

方で、光学走査を応用して実現されるため読み取ることのできる線幅や間隔には限界があり、横方向に平行線を並べるだけのバーコードにおいては個々のコードに持たせられる情報量が10 byte程度に制限され、多くの識別情報を必要とする場合に不向きであった。

このため、利用が拡大するにつれて市場のニーズとして高速認識やコードの汚れによる情報誤りへのロバスト性の確保、あるいは漢字やひらがな、カタカナへの対応など文字種や格納できる情報量の増加などが要求されるようになり、新たなバーコードシステムとして、横方向だけでなく縦方向にもパターンを描き、平面として情報を表現する2次元バーコードが開発された。2次元バーコードは10種を超える仕様が策定されており、大きく分けるとPDF417やコードブロックに代表されるスタック方式とQRコードやCPコード、マキシコード、SPコードに代表されるマトリックス方式がある。いずれの方式においても数センチ角のコードに従来のバーコードを大きく超える容量の情報を格納できる。また、ロバスト性の確保のため誤り訂正コードを用いており、コード面積にして10%程度が汚れて読めなかったとしても記録された情報を読み出すことが可能である。そのため、FA²や物流分野を中心として市場を拡大しつつある。二次元バーコードの例として、(a) PDF417、(b) データ・マトリックス、(c) マキシコード、(d) QRコードのそれぞれについてFigure 1.2に示す。

特に日本ではデンソーが1994年に発表したQRコード[12]が大きく利用されている。近年ではカメラ付き携帯電話の普及に伴い、携帯電話にカメラと連動したQRコード識別ソフトウェアが組み込まれるようになっている。たとえば、名刺に連絡先を記録したQRコードを印刷しておけ

²Factory Automation

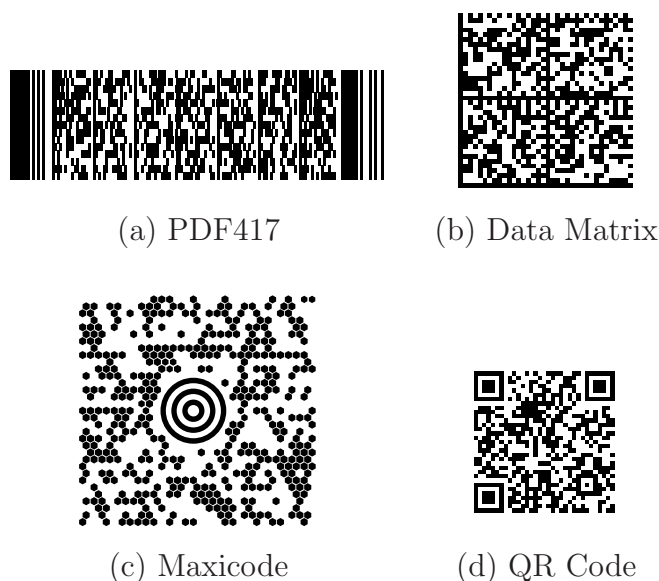


Figure 1.2: 二次元バーコードのパターン例

ば、名刺交換時に携帯電話へ連絡先を登録することが容易にできる。また、街頭ポスターやインターネットで特定のウェブサイトアドレスを記録したQRコードを掲示することによって、携帯電話からウェブサイトへのアクセスがURL³を入力することなく、簡単に行える。このように日本ではFAや物流のみならず、一般消費者を巻き込んだ携帯電話の分野でも利用局面が拡大している。

また、変則的な二次元バーコードにカラーコードがある。他の二次元バーコードが黒と白のピクセルによってのみ情報を表現するのに対して、カラーコードではさまざまな色を用いて描かれるパターンによって情報を表現する。携帯機器のカメラで光学的に取り込んだコードを画像処理することによって埋め込まれた情報が解読される。

しかるに、誤り訂正がシステムとして組み込まれているとはいえ、二次元バーコードも光学走査によってコードを読み取ることに変わりはないので、コードがひどく汚れたり、何かに遮蔽されている状況下では正しく読み取ることができない。また、後述するIC⁴カードやRFIDのように半導体をデータキャリアとする個体識別と比較すると、いったん印刷された情報は書き換えることができず、記録容量も半導体に及ばないの

³Uniform Resource Locator

⁴Integrated Circuit

で、特に低コストを要求される応用分野において今後も利用されていくであろうと著者は考える。

1.2.2 光学文字認識

光学文字認識 (Optical Character Recognition; OCR) は特定の書体で記した文字情報を光学的に読み取る技術であり、1960年代より使われている。バーコード同様、印刷により識別情報を記すことができる一方、バーコードより高密度に記録できるため、より多くの情報を持たせることが可能となる。また、バーコードは見ても何を表すかわからないが、OCRでは見るだけで表している情報を知ることができるという特徴もある。自動化に大きく寄与した技術ではあるが、バーコード同様の光学走査による欠点に加え、読み取るための装置が比較的高価であることから、一般的には使用されていない。

1.2.3 生体認証

生体認証は個人を識別あるいは認証するために、個々人で異なる身体的特徴を用いる方法である。たとえば、指紋・声紋・掌紋・虹彩などを用いるシステムが入室管理などの応用においてすでに実用化されている。専ら個人の特定に用いられ、物品や商品など広義の個体識別としては用いることができない。

1.2.4 磁気カード

磁気カードシステムは磁気ストライプを設けたカードを用いて、その磁気部分に記憶した識別情報をヘッドを介して読み取るものである。鉄道の乗車券・定期券や商店のポイントカードなど種々なカード類に採用されていることから明らかなように、簡単に実現できるシステムとして広く普及している。磁気テープの技術を応用してできるシステムであり、記録内容の書き換えが可能である。しかし、磁気ストライプが露出しているため磁性体に近づけると記録内容が磁氣的に破壊される。また、情報を保持するストライプの経年劣化により情報が失われることもある。さらに、記録内容をカードリーダーによって容易に読み出せるため簡単に偽造できる。これらの理由により、磁気カードはセキュリティ保護を必要とする個人認証などには利用されなくなった。

1.2.5 IC カード

IC カードは半導体メモリを記録装置として用いる電子式のデータキャリアである。単にデータを記憶するだけでなくプロセッサを内蔵することが可能なので、記録されたデータの読み出し時に暗号化など演算を行わせることもできる。このIC カードはリーダに挿入されるとIC カード表面にある金属接点に電氣的な接触が形成され、その接点を通して電力やクロックの供給を受けてデータの授受を行う。一般的にはデータの授受は接点数を減らすためシリアルインタフェースで行われている。

IC カードは耐タンパにすぐれ、データを暗号化して保存することにより、不正アクセスから保護することができる。そのため、金融取引に関するサービスを安全に提供することができる手段として急速に市場に広まりつつある。2002 年度には日本国内だけでも 3,650 万枚の IC カードが発行されており、キャッシュカードやクレジットカードへの採用が多い。また、安全性を高めるために生体認証と IC カードを組み合わせる用いるキャッシュディスペンサーも数多く設置されている。

IC カードの特徴としては、従来の方式と較べて記憶容量が大幅に増加したことがあげられ、その容量は 64 kB にも及ぶ。しかし、電氣的かつ機械的な接触を必要とするため、腐食による接点の劣化や汚れによる読み取り性能の低下が問題とされる。

1.2.6 RFID

RFID システムは上述した IC カードと同様に電子的に情報を格納する。その一方でリーダからの電力供給やデータの授受を物理的な接点を使うことなく無線で行うことで実現される。このため、RFID システムは半導体工学だけでなく無線工学・レーダ工学・電磁気学といった幅広い分野をその礎とする。

RFID システムは Figure 1.3 に示すように、識別する物品に貼り付けるタグ（トランスポンダ）と、それに電力を供給して返ってくる ID データを受信するリーダ、その ID データから何に貼り付けられたタグであるかを照会するためのデータベースの 3 つの主要要素から成る。リーダは一般に高周波の送受信器、制御器とアンテナなどの結合装置から構成される。さらに他のシステムとの接続を可能とするインタフェースを持ち、データベースとの接続に用いられる。一方、トランスポンダは RFID システムの実際のデータキャリアであって、識別に用いる ID データを保持する。

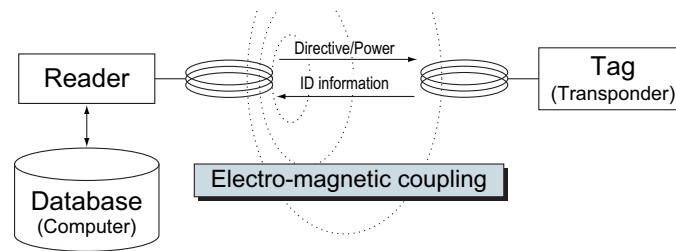


Figure 1.3: RFID システムの構成

これは結合装置とマイクロチップから構成される。トランスポンダは通常、独立した電源を内蔵していないので、リーダとの交信が可能な領域に入るまでは休眠状態にある。すなわちリーダから電力供給を受けてはじめてトランスポンダは活性化され、データの授受が行われる。

このような RFID システムは、他の個体識別システムと較べて多くの優位点を持つ。まず第 1 に、記憶素子として半導体メモリを用いており、半導体製造プロセスの微細化に伴う集積度の増加によって、IC カードと同様に広大な記憶容量が実現できる。第 2 に、表面に露出した接点を持たないために劣化や汚れ、遮蔽による影響が起りにくい。接点を介してプローブすることができないため耐タンパも高い。第 3 に、情報は無線通信によって行われるのでリーダに接近させるだけで情報が授受でき、ユーザの利便を損なわないばかりか、他の個体識別技術で必要とされる正確な位置あわせが要求されないため、識別処理の自動化が容易である。そのため、群ロボットや車両、あるいは実験動物といった移動体がどのリーダの識別空間に存在するかを把握することによって、これらの管理を自動化することが可能である。ただし、金属から構成されるような物品や水分を多く含む生体においては情報伝送に用いる電磁波の周波数によって到達距離が大きく異なるため、システムの設計時に十分な注意が必要である。第 4 に記憶素子として磁気抵抗メモリ (Magnetoresistive RAM; MRAM) や強誘電体メモリ (Ferroelectric RAM; FeRAM) あるいは Electronically Erasable and Programmable ROM (EEPROM) のような不揮発メモリ (Non-Volatile RAM; NVRAM) [13, 14] を内蔵させることができるので、これによって情報の書き換えが可能となり、特に流通経路の調査を可能とするトレーサビリティの観点から、食品業界において注目がなされている。

以上の理由から RFID システムは現在、普及に向けて急激に市場が立

ち上がりつつある。実際の応用例としては鉄道の運賃収受システムや高速道路の通行料収受システムが挙げられる。また、紙に漉くことができる極小型のトランスポンダも開発されており [15]、有価証券の真偽判定など多岐にわたる分野で期待が高まっている。IC カード同様、マイクロプロセッサを内蔵することができるため [16]、特に暗号化を伴う無線伝送によって耐タンパ性を高めることができ、伝送情報の盗聴、トランスポンダの偽造、あるいは内容の変造が困難である [17]。そのため、電子マネーや入室管理のようなセキュリティを必要とする応用でも積極的に受け入れられつつある。一方で、リーダさえあれば直接接触させなくても近傍に近づいただけで情報が読み取れてしまうため、権限のないリーダが情報を剽窃することのないよう相互認証などの個人情報保護の仕組み [18–20] が必要とされている。

また、非接触かつ自動で高速に物品を識別できることから RFID を物流や流通に応用する動きが活性化している [21]。たとえばマサチューセッツ工科大 (Massachusetts Institute of University; MIT) が中心となって設立された Auto ID Center ではバーコードの置き換え技術として RFID を研究している [22]。具体的には、トランスポンダを識別対象の物品に貼り、一意の ID をあらかじめ割り当てる。物品ごとに固有の ID がデータベースに登録され、物流拠点を通るたびに照合され物品がロストしていないかを確かめられる。最終的に小売店に到着し、在庫管理や会計処理に用いられる。このように市場を流通するほぼ全ての商品に印刷されているバーコードを完全に置き換えることができるとすれば、RFID 業界は非常に大規模な市場を手にいれることができる。しかるに、現時点では RFID をバーコードの置き換え技術と見たときに、解決しなくてはならない問題が二つ存在する。

一つはトランスポンダのコストである [23]。印刷するだけで完成するバーコードと異なり RFID は半導体技術を応用しているため、認識対象に貼り付けるためのトランスポンダを製造するためには莫大な投資が必要である。製造コストの削減については、リーダからの供給電力を整流せずに AC のまま直接用いることで実装面積を削減する回路方式 [24] が提案されている。また、有機トランジスタを用いた実装方式 [25–27] も注目を浴びている。導電性高分子の実現に伴って可能となった技術であり、インクジェットプリンタで印刷してつくることができるために、安価にトランスポンダを実装するための技術として期待されている。

もう一つは衝突の問題であり、無線を用いて通信を行う RFID におい

て複数のリーダーやトランスポンダが存在する環境では、相互干渉によって正常な識別処理が妨げられるため、これを防ぐ技術が必要とされる。特に独立電源を持たないパッシブ・トランスポンダを用いる RFID では回路の低消費電力化を視野にいたした通信方式 [28]、アーキテクチャ [29–31]、ならびに回路の実現方法 [32–36] を考案する必要がある。

1.3 RFID における衝突問題

RFID は無線技術を用いてリーダーとトランスポンダが非接触通信することによって個体識別を行う。もし、リーダーとトランスポンダがそれぞれ唯一に存在するのであればノイズなどの外乱を鑑みない限り通信は成功し、物品を完全に識別することができる。しかるに、物流や流通における応用を考慮すると必ずしもこの前提は成立しない。そのため、複数のリーダーまたは複数のトランスポンダが存在して互いの通信に干渉を引き起こす [37]。これを RFID では応答の衝突と呼び、解決を図るべき問題として取り上げられている。この衝突問題は大きく分けて二つに分類することができる。すなわち、複数のリーダーが近傍に存在することによって相互に干渉することで、トランスポンダの応答が認識できなくなる衝突と、複数のトランスポンダが単一のリーダーに対して同時に応答することによる衝突である。本節では、これらの要因で引き起こされる衝突について説明する。

1.3.1 複数のリーダーが近傍に存在することによる衝突

リーダーはそれぞれ、識別可能領域 (Interrogation Zone) と呼ばれる空間を持っている。この範囲内にトランスポンダが存在すると、電磁誘導により電力が与えられてトランスポンダが活性化し、ID データを送り返すことで認識処理がなされる。このとき複数のリーダーが近傍に存在すると、電力供給のための輻射電波または識別可能領域の重複が原因となる干渉が発生し、トランスポンダの応答が正常に受信できない。

一般的に、リーダーはトランスポンダと較べて多大なる演算資源を利用することができるので、さまざまな解決手段が考案されている。たとえば干渉による衝突をコスト関数と捉え、これを最小化する問題を考えれば、ニューラルネットワーク [38] やシミュレーテッドアニーリング [39]、遺伝的アルゴリズム [40]などを適用することで解決を図ることが可能である。そ

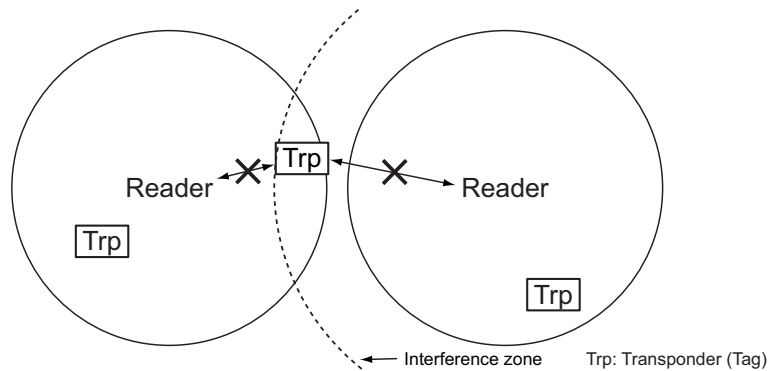


Figure 1.4: 隣接するリーダによる電磁干渉

のほかにも Frequency Division Multiple Access (FDMA) や Time Division Multiple Access (TDMA)、Carrier Sense Multiple Access (CSMA) のような一般的な多重化手法を用いることによるチャネル衝突の回避が図られることもある。

本節では、干渉の原因として電力供給波による妨害と識別可能領域の重複による通信の衝突についてそれぞれ分析するとともに、代表的なリーダ同士の衝突防止アルゴリズムとして、Colorwave、HiQ、PULSE について解説する。

1.3.1.1 隣接リーダの電力供給波による干渉

この衝突は Figure 1.4 に示されるように、隣接するリーダ同士で起きる通信障害である。リーダはトランスポンダに電力を供給するために強大な電波を輻射している。トランスポンダの出力はリーダと較べて微弱であるため、リーダの識別可能領域はトランスポンダの応答が到達する範囲に制約される。一方、リーダの電力供給波は出力が大きいので識別可能領域よりも到達範囲が広い。これを干渉範囲とすると、隣接するリーダの干渉範囲にいるトランスポンダによる応答は、トランスポンダが識別可能領域に入っているにもかかわらず他のリーダによる輻射電波の影響を受けて認識することができない。

この衝突を解決するためには、リーダがトランスポンダに電力を供給するための輻射電波が隣接リーダの識別可能領域に影響しないような手段を講ずる必要がある。たとえば、物理的な解決策としては電力供給波の到達範囲を考慮してリーダの設置を考慮する、あるいは電力供給波が

識別可能領域外に漏れ出さないように領域の境界で電磁遮蔽を実施するといった手段があげられる。また、近傍にあるリーダが同時にトランスポンダと通信や電力供給しないように制御するアルゴリズムでの解決も行われる。

1.3.1.2 識別可能領域が重複することによる干渉

Figure 1.5に示すように、複数のリーダが近傍に存在して識別可能領域が重複していることを考える [41]。このとき、重複する領域内にあるトランスポンダにおいてはリーダからの応答要求が衝突する。したがってトランスポンダは応答要求を解釈することができないため、これに応答することもできない。また、応答開始をトリガ信号で要求するような RFID においては、トランスポンダはトリガに対して応えることができる一方で、近傍するリーダのタイミング同期が完全にとられていなければ、トランスポンダの応答をリーダが正常に解釈できない。つまり、トランスポンダの応答は最初のトリガが受信された時点で開始されるが、このとき最初にトリガを輻射したリーダを除いてはトリガを輻射するまでの応答データを喪失することになる。また、トリガによる応答への妨害も考えられる。このような場合、リーダはトランスポンダを認識できない。

この衝突を解決するためには、識別可能領域が干渉しないようにリーダを設置するか、あるいは識別空間に対する外部との電磁遮蔽を完全に行うなどの方法によって物理的に解決を行うことができる。また、リーダとトランスポンダの通信動作をリーダごとに別の通信チャネルで行わせることによるアルゴリズムレベルでの解決を図ることも可能である。

1.3.1.3 Colorwave

Colorwave はグラフの色分け問題に着想を得たアルゴリズムである [42, 43]。リーダ同士の衝突防止を考慮するにあたって、隣接するリーダが接続されたグラフを考え、これを隣り合うノードが同じ色にならないように色分けすることで衝突回避するものである。

Colorwave では TDMA のような一般的な通信の多重化手法を用いる。まず始めに TDMA のチャネルであるスロットに Figure 1.6 のように一意の色を割り当てる。言い換えると、同じ色を割り当てられたスロットは二つと存在しない。リーダは通信を始める前に自分の色をランダムで決定づける。その自分の色に一致するスロットで通信を行い、一致しないスロットでは電波輻射を停止する。この手法は、多重通信として TDMA

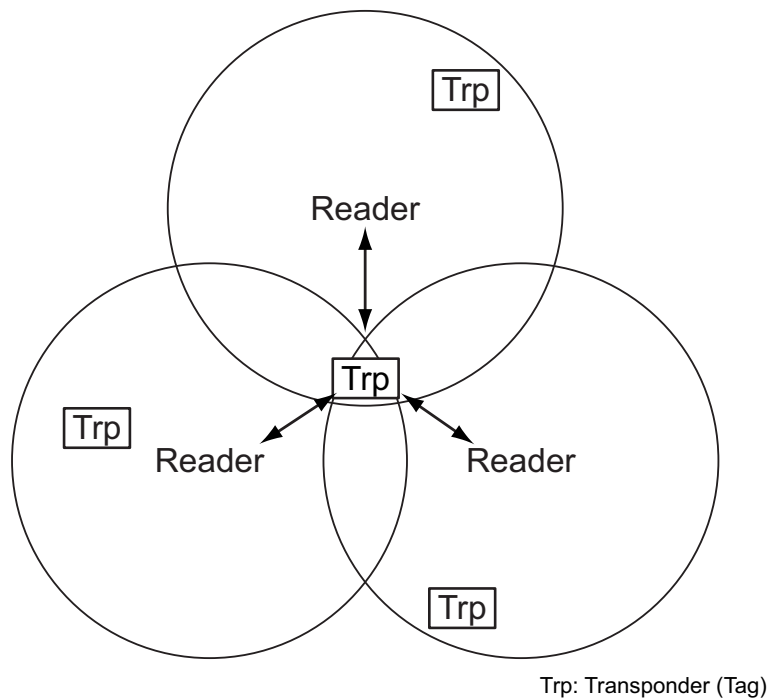


Figure 1.5: 複数のリーダによる通信の衝突

に基づいており、リーダがスロットをランダムに選んで送信することから、s-ALOHA⁵の一種である。一方、リーダがランダムで色付けすることは偶然同じ色を選んでしまうリーダが複数存在する確率はゼロにできない。s-ALOHA と異なる点は、この偶然起きてしまった衝突の回避にある。Colorwave では、トランスポンダとの通信が許される期間のほかに kick 期間と呼ばれる折衝のための期間が色別に用意されている。リーダが他のリーダと衝突していることを検知すると、トランスポンダとの通信を取りやめ、近傍のリーダを kick する。kick されたリーダはランダムで色を割り当てなおす。通信が衝突する可能性のあるリーダのみ kick されるので、この動作によって色分け問題が解決する方向に収束する。Colorwave には色数を固定とする Distributed Color Selection (DCS) と可変とする Variable DCS (VDCS) があるが、後者は特にリーダとトランスポンダの通信が行われる頻度が大きく変化する環境において有効であることが確かめられている。

⁵Slotted ALOHA

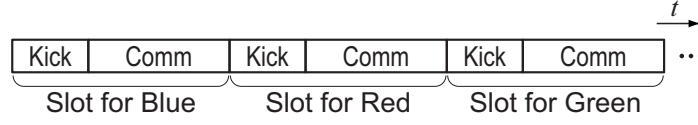


Figure 1.6: Colorwave のスロット構成

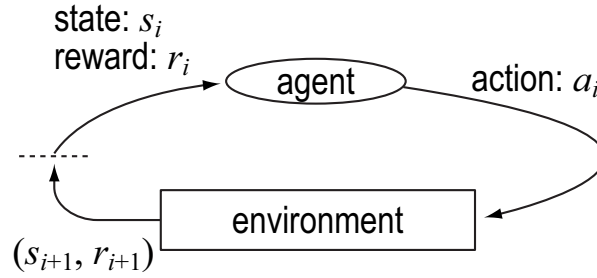


Figure 1.7: 環境によるエージェントの強化学習

1.3.1.4 HiQ

Hierarchical Q-learning (HiQ)[44, 45] とは、その名が示す通り階層的に構成された Q-learning システムによって通信スロットの割り当てを最適化することにより衝突を回避するものである。Q-learning [46] は強化学習の一種である [47]。Figure 1.7は、Q-learning の構成要素であるエージェントと環境の相互作用を模式的に表す。エージェントと環境は各離散時間ステップ $t = 0, 1, 2, \dots$ において相互的に作用する。それぞれの時間ステップ t においてエージェントは環境の状態を表す値 $s_t \in S$ を受け取る。ただし、 S は環境の持つ状態集合である。 s_t に基づいてエージェントは行動 $a_t \in A(s_t)$ を選ぶ。ここで、 $A(s_t)$ は s_t において可能な行動の集合である。時間ステップが 1 経過すると行動に応じた報酬 $r_{t+1} \in R$ と新しい状態 s_{t+1} が与えられる。Q-learning におけるエージェントの目的は累積した報酬 $r_t = r(s, a)$ が最大となるような状態に対する行動 $\pi(s, a)$ を発見することである。

この HiQ も TDMA に基づいてリーダとトランスポンダの通信を制御する。リーダ群は Figure 1.8に示すように階層的な構造をしており、リーダ、R サーバと Q サーバから構成される。末端に存在するリーダは、直上の R サーバによって割り当てられたスロットを使用してトランスポン

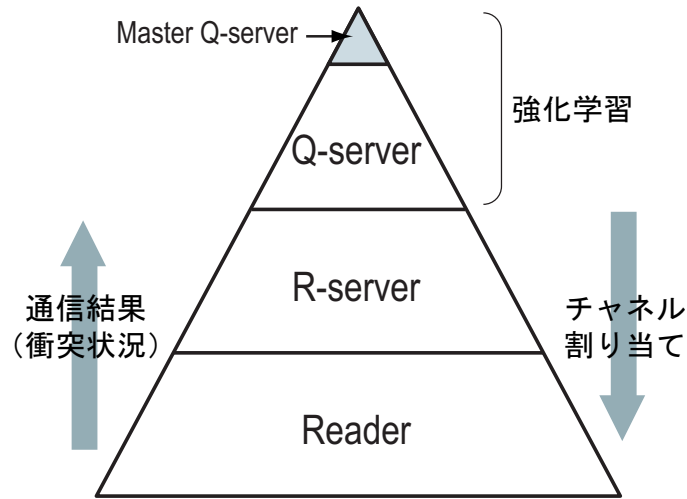


Figure 1.8: HiQ アルゴリズムにおけるリーダ群の階層構造

ダとの通信にのみ専念する。すなわちリーダは衝突を回避するための動作を何一つ行わず、他のリーダとの衝突を検知した場合のみ R サーバに衝突検知を報告するのみにとどまる。R サーバは中間に存在し、Q サーバによって割り当てられたスロット資源を直下のリーダに分配する働きをする。Q サーバは階層の最上位に位置し、大域的にスロット群を直下の R サーバに割り当てる。HiQ では、この割り当て数を Q-learning による強化学習で最適化することにより衝突を回避する。最上位の Q サーバから下位に向けてスロットの割り当てを細分化していくことによって局所的な最適化にとどまらず、リーダ群の全般にわたる最適解を求められる手法であるといえる。また、強化学習に基づくアルゴリズムであるので、最適解に達するまでに若干の遅れはあるものの、適応的にリーダ数の変化に対応できる方式である。

1.3.1.5 PULSE

Colorwave や HiQ のような TDMA に基づく手法と異なり、PULSE は CSMA に基づくアルゴリズムである [48]。無線伝送で CSMA を実現するためにビーコン信号を用いる。このビーコンを輻射するためには制御用の通信チャンネルが別途必要である。この方式に基づくリーダは三つの状態を遷移しながら通信を遂行する。まず、通信を開始したいリーダは WAIT 状態に移行する。この状態では制御チャンネルをモニタして他のリーダによ

るビーコンが傍受できないことを確認する。確認ができればCONTENTD状態に移る。これは、複数のリーダが同時に通信を開始しようとして衝突することを防ぐために配置される状態であり、リーダはランダムな期間において、さらに制御チャンネルをモニタする。ランダムな期間を経過してもなおビーコンが傍受されない、すなわち他のリーダが通信していないと判明すれば、ビーコンを制御チャンネルに輻射し始め、トランスポンダとの通信を開始する。この手法は単純であることから容易に実装可能である一方、リーダ数が増大すると衝突の回避のためにWAIT状態にいるリーダが常に複数存在するようになり、通信効率の低下を避けることができない。

1.3.2 複数のトランスポンダとリーダの衝突

リーダの識別可能領域内に複数のトランスポンダが存在すると、Figure 1.9に示すように、リーダの応答要求に対して領域内の全てのトランスポンダが応答しようとして通信障害が引き起こされる。これは複数のトランスポンダと単一のリーダによって引き起こされる衝突と分類される。リーダとリーダの干渉による場合と異なり、トランスポンダは電磁結合により給電されているため、消費電力を非常に小さく抑えなければならない。また、実装性を高めて同時に製造コストを下げるため、回路面積についても著しい制限がある。以上の理由により、トランスポンダ同士の衝突は可能な限り簡素な方式で行われる必要がある。本論文で解決の目標とする衝突は、この複数のトランスポンダが同時応答することによるものである。

1.4 従来研究

前述のとおり、RFIDには単一のリーダに対して複数のトランスポンダが同時応答することによって通信が衝突し、トランスポンダの識別ができない問題が存在する。これは特に物流や流通、販売への応用を考慮したときに顕著になる。これらの分野においては識別すべき物品の種別が多いため、できる限り高効率に識別したいという要求があるにも関わらず、この輻輳問題のためにトランスポンダを個別に識別するのであれば、業務効率を著しく低下させRFID導入による利点を失ってしまう。そこで、これまで複数リーダによる衝突問題とは別に、複数トランスポンダの輻輳による衝突を回避するアルゴリズムが研究されてきた[49–51]。ト

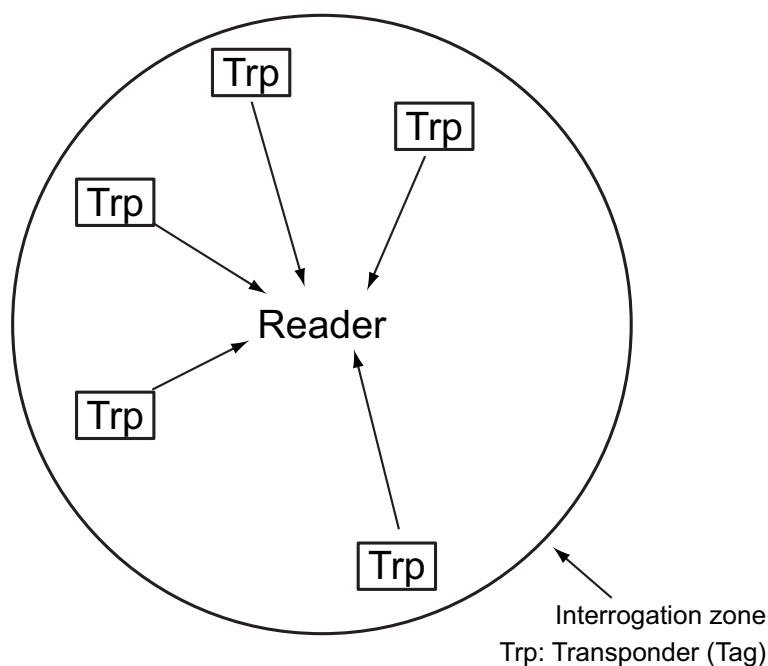


Figure 1.9: 複数のトランスポンダと単一のリーダ間における衝突

ランスポンダの回路規模や消費電力は厳しく制限されているために、可能な限り簡素で回路化が容易であることが重視される。これを満たすトランスポンダ向け衝突防止アルゴリズムは、決定的手法 (Deterministic algorithm) と 確率的手法 (Stochastic algorithm) の二種類のいずれかに分類される [51]。

1.4.1 決定的手法による衝突防止

決定的手法とは、最終的には全てのトランスポンダが完全に識別されることを保証できる衝突防止アルゴリズムを示す。具体的には、個々のトランスポンダに対して順番にIDを問い合わせ、IDデータを1ビットずつ確定する。識別可能領域に存在する全てのトランスポンダに対して問い合わせを終えたとき、識別処理が完了する。つまり、リーダはその全トランスポンダのIDを獲得できたことになる。完全な識別を担保する代償として、識別にかかる時間が長いという欠点が存在する。リーダが個別に問い合わせる必要があるために、識別時間は低速にならざるを得ない。アルゴリズムレベルでの工夫により多少は高速化できるとはいえ、識別領域

に存在するトランスポンダ数やIDデータのビット長に比例して識別時間が長くなる。具体的には、決定的手法により実現可能な識別速度は単一のリーダにおいて高々毎秒100個程度である。したがって流通分野で期待されているSupply-Chain Management (SCM) やInventory Management System (IMS) のような高速かつ高効率に大量の物品を識別する必要のある応用分野に対して決定的手法は不適合である。一方で、確実に全てのトランスポンダを識別することができるため、効率よりも安全性や信頼性が優先される分野、たとえば電子マネーや鉄道の改札などにおいては決定的手法が適用される。

トランスポンダへの問い合わせを漏れなく効率的に行うために、決定的手法によるアルゴリズムは、ほぼ例外なくツリー構造を用いている [52–56]。特に二分木を用いてIDのビット位置ごとに“0”と“1”に分けることで、IDの取りうる全空間を表現することができる。このとき、木の深さはビット長と等しい。どのように木を効率的にトラバースするかという点が、決定的手法によるアルゴリズムの重要な性能指標となる。この決定的手法に分類されるアルゴリズムとして、

- Bit-by-bit
- Binary Search
- Binary Tree
- Query Tree

があげられる。また、効率を向上させるための工夫をこれらに適用した改良アルゴリズムとして、

- Adaptive Binary Splitting
- Query Tree の改良
 - aggressive advance
 - shortcutting
 - Query Tree short long
 - Query Tree incremental matching
- Hashed Query
- Bin-Slotted Hybrid Search

がある。そこで、本節ではこれらのアルゴリズムについて順番に説明を加える。

1.4.1.1 Bit-by-bit

Bit-by-bit は決定的手法の中で、もっとも単純であり、それゆえもっとも非効率なアルゴリズムである [57, 58]。リーダーはトランスポンダに対する指令として REQ n と SLP n, i 、RST がある。各指令の定義は以下の通りである。

- REQ n : ビット位置 n にある ID データビットの応答を要求する
- SLP n, i : ビット位置 n の ID データビットが i であるトランスポンダの応答を無効にする
- RST: 無効にしたトランスポンダを有効に戻す

この指令体系において、リーダーはビット位置をインクリメントしながらトランスポンダの応答を要求する。トランスポンダは要求された位置にある ID ビットを単純に送り返すだけである。衝突しなければ、二分木における分岐方法は単に応答のあったビットに確定される。一方、もし衝突が起こった場合はそのビット位置が “0” と “1” であるトランスポンダが、それぞれ少なくとも一つ以上存在するということであるから、そのビット位置をスタックに保存し、“1” のものを無効化した上で “0” のものについて次のビットを調べる。衝突のたびに無効化が行われ、最終ビット位置まで到達した際に一つのトランスポンダの識別が完了する。

たとえば、ID が $N \in \{0101, 0110, 1011, 1100\}$ の四つのトランスポンダを識別する場合を考える。この N における ID ビット長は 4 ビットであり、したがって二分木の深さは 4 である。Figure 1.10 にリーダーがたどるべき二分木を示す。また、Figure 1.11 にリーダーとトランスポンダ群の間で交される指令と応答の一部を掲載する。ここで、Figure 1.10 において木の深さはトランスポンダ ID のビット位置を表しており、各節点ではそのビット位置における ID データが “0” のものは左に、“1” のものは右に枝分かれする。また、丸囲みの数字は認識順であり、この順序にしたがって木構造を矢印の方向に沿って探索する。以降の木構造図も同様である。

まず、リーダーは ID データの 1 ビット目を要求する。すると ID データの 1 ビット目はそれぞれ “0”、“0”、“1”、“1” であるので応答は衝突する。したがってリーダーは 1 ビット目が “1” のものを無効にし、“0” のもののみ有効にする。次の 2 ビット目は “1” のものしかないので、“1” が確定する。3 ビット目で再び衝突するので、“1” を無効にして “0” のみ応答させる。4 ビット目の要求指令で 0101 が確定する。続く識別対象は 1 ビット目は “0” で、かつ 3 ビット目で “1” であったトランスポンダである。そこ

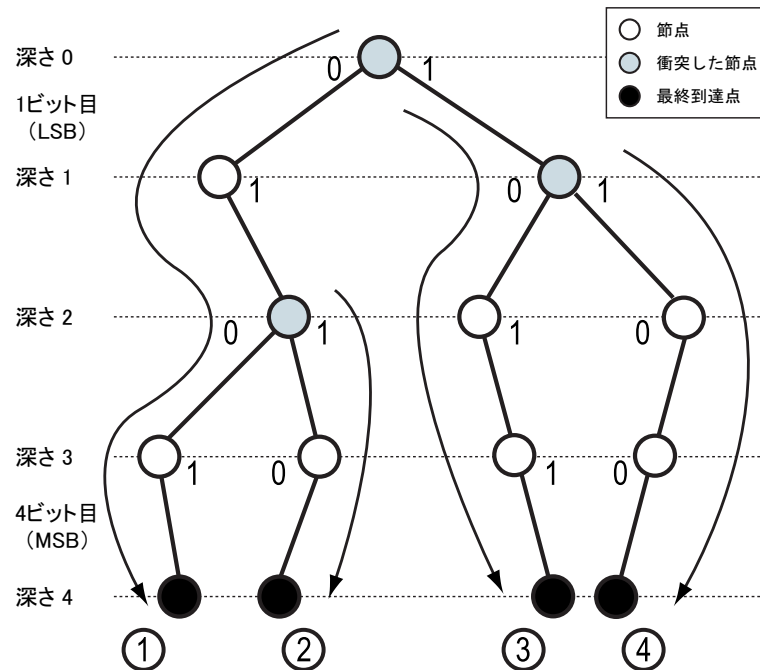


Figure 1.10: Bit-by-bit アルゴリズムの木構造

で、1ビット目が“1”であるもの、3ビット目が“0”であるものを順番に無効にし、4ビット目を要求して0110が得られる。このように、衝突と無効化を繰り返し、最終ビットに至る認識を全ての衝突が解決するまで繰り返せば、全トランスポンダのIDが確定する。効率を改善するため後述の Binary tree アルゴリズムと組み合わせた提案もなされている [59]。

1.4.1.2 Binary Search

Binary search (BS) 法はIDの範囲を徐々に絞っていくことによりトランスポンダを識別するアルゴリズムである [51, 60]。リーダーはトランスポンダに対する指令としてREQ min,maxのみが定義されている。これはIDデータがmin以上max以下であるトランスポンダにのみ応答を要求するコマンドである。このとき、IDがREQ指令に与えられた範囲内にあるトランスポンダのみがIDを送信する。そのため、リーダーは受け取ったIDの衝突状況から新たな範囲を与えることができ、これによって徐々に衝突が回避される。

この指令体系では、リーダーは二分木の中で最も根に近い衝突ノードで

指令	#1	#2	#3	#4	受信応答	
REQ, 0	0	0	1	1	C	
SLP, 0, 1	—	—	Sleep	Sleep	Z	
REQ, 1	1	1	N/A	N/A	1	
REQ, 2	0	1	N/A	N/A	C	
SLP, 2, 1	—	Sleep	N/A	N/A	Z	
REQ, 3	1	N/A	N/A	N/A	1	0101
RST	Act.	Act.	Act.	Act.	Z	
SLP, 0, 1	—	—	Sleep	Sleep	Z	
SLP, 2, 0	Sleep	—	N/A	N/A	Z	
REQ, 4	N/A	0	N/A	N/A	0	0110

以下省略

Figure 1.11: Bit-by-bit による認識フロー例

調査範囲を二分して細分化する。細分化した範囲で応答要求を繰り返し、最終的に衝突がなくなれば識別が完了する。トランスポンダはIDが範囲内にあるかどうかを確認するための比較ロジックが必要であるが、状態遷移を伴う必要がないので実装面積は比較的小さく抑えることができる。

ここで、 N で表される ID 群について BS による認識動作を例示する。この場合の二分木を Figure 1.12 に示す。他の決定的手法と異なりはじめから木全体を意識して処理を進める必要があるため、図には存在しないノードも描いてある。Figure 1.13 はトランスポンダとリーダーの間で交わされる通信の全容を示す。まずはじめに、木全体を対象として応答を要求する。つまり、0000 から 1111 までを範囲とする REQ を発行 (Figure 1.12(1)) する。このとき、全トランスポンダが応答するため、応答は全ビットにわたり衝突する。これは、根ですでに “0” と “1” に二分していることを表しているから、まず根で範囲を二分する。ここでは、0000 から 0111 までと、1000 から 1111 まで (Figure 1.12(2)) とする。ここで 0000 から 0111 までの REQ は 01CC という応答を得る。下位二ビットが衝突しているということを表すので、範囲をさらに 0000 から 0101 まで (Figure 1.12(3)) と、0110 から 0111 まで (Figure 1.12(4)) に二分する。結果として 0101 と 0110 が順番に認識される。一方、1000 から 1111 までの範囲を調査する (Figure 1.12(5)) と、これも下位三ビットが衝突した応答が得られる。このため、1000 から 1011 まで (Figure 1.12(6)) と 1100 から 1111 まで (Figure 1.12(7)) に二分して、1011 と 1100 が得られ、認識処理が完了する。

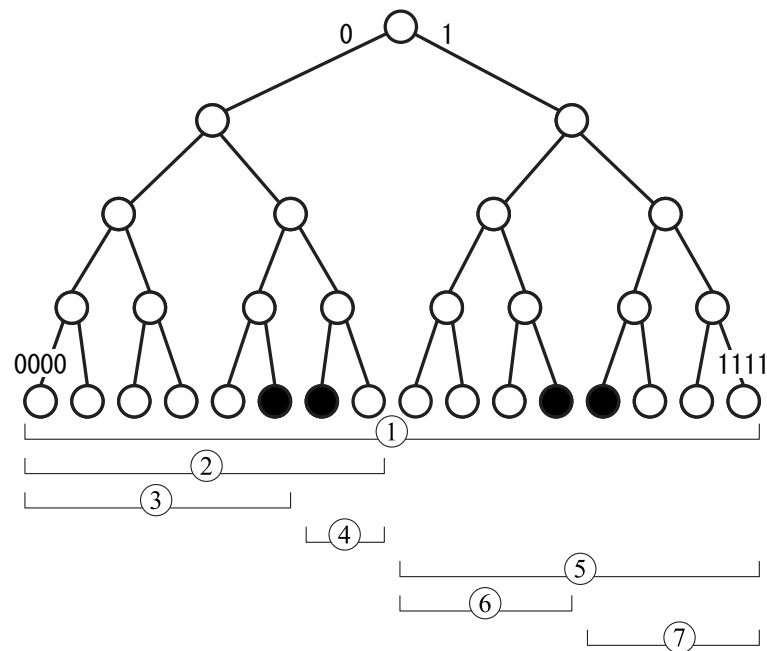


Figure 1.12: Binary search アルゴリズムの木構造

1.4.1.3 Binary Tree

二分木に沿ってインクリメンタルにマッチングを行い、探索対象を絞る方法として Binary Tree (BT) 法があげられる [50, 51, 61–64]。リーダーとトランスポンダはそれぞれ現在探索中の木の深さをカウンタで保持している。そのため、このアルゴリズムではトランスポンダが状態遷移して応答できるかできないかを決定する必要がある。リーダーには REQ, i 指令が定義されている。これは、現在カウンタが示すビット位置における ID データが i であるトランスポンダのみに応答を要求し、一致しないものに以後の応答を禁止する指令である。応答を禁止されたトランスポンダは、次に RST 指令が与えられるまではリーダーのいかなる指令にも応答しない。

REQ 指令が与えられると、各トランスポンダはカウンタの示すビット位置を調べて、指令と一致すれば次のビット位置にある ID データビットを応答する。衝突が検出されれば、リーダーはそのカウンタ値をスタックに保存しておき、ひとまず “0” として探索を継続する。全ての ID ビットが確定すれば、スタックにあるビット位置が “1” の場合を探索する。このアルゴリズムにおいても、全ての衝突が解決できたとき探索を終えること

指令	#1	#2	#3	#4	受信応答	
REQ, 0000, 1111	0101	0110	1011	1100	CCCC	
REQ, 0000, 0111	0101	0110	N/A	N/A	01CC	
REQ, 0000, 0101	0101	N/A	N/A	N/A	0101	0101
REQ, 0110, 0111	N/A	0110	N/A	N/A	0110	0110
REQ, 1000, 1111	N/A	N/A	1011	1100	1CCC	
REQ, 1000, 1011	N/A	N/A	1011	N/A	1011	1011
REQ, 1100, 1111	N/A	N/A	N/A	1100	1100	1100

Figure 1.13: Binary search による認識フロー例

ができて、その時点で全トランスポンダの ID 獲得が完了したといえる。

同様に N で与えられるトランスポンダ群に対する BT による識別動作を例示する。Figure 1.14は二分木を表したものであり、Figure 1.15は認識動作におけるリーダーとトランスポンダ間の通信を模式するものである。まず、RST 指令によって全てのトランスポンダを応答状態にする。同時にリーダーとトランスポンダ双方に内蔵されているカウンタがリセットされる。次の REQ, 0 指令はカウンタ値のビット位置、すなわち 1 ビット目の ID ビットが “0” のトランスポンダのみに 2 ビット目の ID ビットを応答させる。トランスポンダ #3 と #4 は “0” でないので応答しない状態に遷移する。#1 と #2 による応答がともに “1” であるので、次の応答要求は REQ, 1 である。この時点で #1 と #2 の 3 ビット目の値が異なるため、応答は衝突する。よってリーダーはひとまず 3 ビット目が “0” であるトランスポンダの識別を続行する。これにより #1 の 0101 が識別される。リーダーは次の ID を確定するため、RST を発行してから先ほど同様の操作を繰り返し、今度は 3 ビット目が 1 のものを応答させる。このように二分木を深さ優先探索していくことで、全てのトランスポンダをインクリメンタルに認識することができる。

Adaptive Binary Splitting BT ではトランスポンダ ID の分散によってスループットが変化する。すなわち、二分木のどちらかに偏っているような ID 群では衝突が明らかに増加し、そのためトランスポンダの応答が無駄になる。これを防ぐためにできるだけ均等に分散するように二分木を構成する手法として Adaptive Binary Splitting (ABS) アルゴリズムが考案された [65, 66]。ABS では ID ビットの代わりにランダム値を用いる。リーダーに定義される指令には REQ、COL と ACK がある。このアルゴリズムのポイントとしては、リーダーがトランスポンダに先ほどの通信が衝

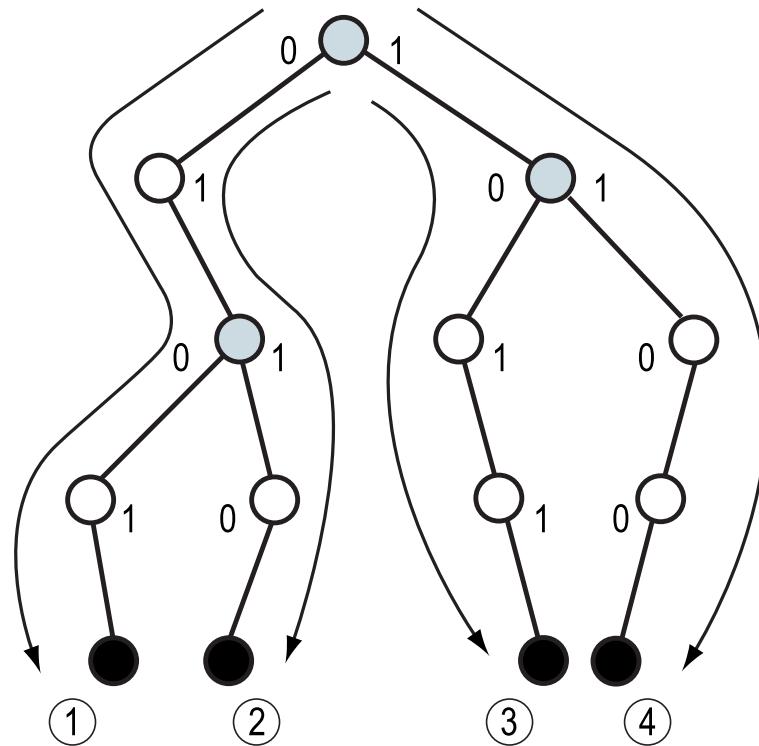


Figure 1.14: Binary tree アルゴリズムの木構造

突したかどうかを通知するための COL 指令が存在することにある。トランスポンダは待機カウンタを持っていて、次に応答を許されるまでに受信すべき ACK 指令の数が格納される。リーダーが REQ 指令を送信すると待機カウンタが 0 のトランスポンダは ID を応答する。このとき、応答が衝突していればリーダーは COL 指令を送出してトランスポンダに衝突したことを通知する。COL 指令を受け取ったトランスポンダは直ちにランダム生成器を利用して乱数生成を行う。生成した乱数が 0 のものは続く REQ に応答することができる一方、1 のものは待機カウンタに 1 を加え、ACK を受信するまで応答できない。待機中のものは COL を受信すると待機カウンタに 1 を加えて待機期間を延ばす。この操作を繰り返して応答可能なトランスポンダが唯一になれば、その ID を獲得することができたことになるので、リーダーは ACK を発行して受信できたことを通知する。ACK を受信すると、待機カウンタが 0、すなわち認識に成功した ID を持つトランスポンダは応答を停止する。待機カウンタが 1 以上のものはカウンタをデクリメントして次の識別処理に備える。

指令	カウンタ	#1	#2	#3	#4	受信応答	
RST	0	Act.	Act.	Act.	Act.	Z	
REQ, 0	0	1	1	N/A	N/A	1	
REQ, 1	1	0	1	N/A	N/A	C	
REQ, 0	2	1	N/A	N/A	N/A	1	0101
RST	0	Act.	Act.	Act.	Act.	Z	
REQ, 0	0	1	1	N/A	N/A	1	
REQ, 1	1	0	1	N/A	N/A	C	
REQ, 1	2	N/A	0	N/A	N/A	0	0110

以下省略

Figure 1.15: Binary tree による認識フロー例

指令	#1		#2		#3		#4		受信応答
	応答	待機	応答	待機	応答	待機	応答	待機	
REQ	0101	0	0110	0	1011	0	1100	0	C
COL	—	0	—	1	—	1	—	0	Z
REQ	0101	0	Wait	1	Wait	1	1100	0	C
COL	—	1	Wait	2	Wait	2	—	0	Z
REQ	Act.	1	Wait	2	Wait	2	1100	0	1100
ACK	Wait	0	Wait	1	Wait	1	Sleep	—	Z
REQ	0101	0	Wait	1	Wait	1	Sleep	—	0101
ACK	Sleep	—	Act.	0	Act.	0	Sleep	—	Z

以下省略

Figure 1.16: Adaptive binary splitting の認識フロー例

Figure 1.16にID群 N に属するトランスポンダの認識例を示す。COLおよびACK 指令に伴って待機カウンタの値が増減していることがわかる。乱数生成機構を用いるものの、このABSでは衝突が回避されるまでトランスポンダが通信を待機するため、最終的に全てのトランスポンダの認識を保証することができる。

1.4.1.4 Query Tree

Query Tree (QT) 法は特定のプレフィックスを指定して応答すべきトランスポンダを制限することで、最終的に一つのトランスポンダIDを識別するアルゴリズムである [50, 62–64, 67]。衝突が発生した場合、プレフィックスの末尾に“0”ないし“1”を追加して絞り込みを行う。衝突が回避されるまでリーダはプレフィックスの末尾への追加を続ける。そのため、QTでは指令としてREQ, P が定義されている。ただし、 $P = p_0p_1 \cdots p_n, n$

はプレフィックス長で $p_i \in \{0, 1\}$ を満たす。トランスポンダとしてはプレフィックスに合致するかを ID の MSB から導出するためのロジックが必要であるが、状態遷移を必要としない。プレフィックスに ID が合致するとトランスポンダは ID を応答する。QT も探索対象の追跡に二分木を利用する。衝突があれば、まずプレフィックスに “0” を加えて探索を行い、のちに “1” を加えて探索する。木全体を探索し衝突が解決できていれば識別処理の完了である。

ID 群 N における識別処理の二分木を Figure 1.17 に、通信例を Figure 1.18 に示す。REQ, ϵ は全ての ID が応答の対象であるため、結果は全ビット衝突する。そこで 1 ビット目が “0” の ID のみに絞り込むため、プレフィックスを “0” とする。REQ, 0 指令には 0101 と 0110 が応答するため、結果はやはり衝突が検知される。そこでプレフィックスである “0” に “0” を追加して 00 とする。このプレフィックスを持つ ID は存在しないので応答は得られない。次にリーダーは “0” に “1” を追加し 01 のプレフィックスについて応答を要求する。今度は 0101 と 0110 の両方から応答があり、また衝突が起きる。リーダーはこれに “0” を追加し 010 の応答を要求し、これによって 0101 が識別される。このようにプレフィックスを徐々に長くしていくことで探索対象を減らし、最終的に単一のトランスポンダに到達する。

QT には無駄な通信が多いため、スループットの向上が望めない。たとえば毎回トランスポンダは ID を全ビット応答するが、衝突を起こすプレフィックスでは衝突しているかいないかという情報のみが必要であり、全ビットを送信しても判別できないため有効に活用できない。また、リーダーが送出する REQ 指令についてもプレフィックスに応じて長くなるため、木を下っていく段階では追加されたプレフィックス値以外は無駄である。これらの不必要な通信を廃して効率を改善するために、アルゴリズムの工夫や改良がいくつか提案されている。軽微な工夫として aggressive advance と shortcutting を、またアルゴリズムの改良として QT-sl、QT-im と HQ を紹介する。

aggressive advance aggressive advance は、QT においてあるプレフィックスで衝突が起きたとき、末尾に “0” と “1” を追加するのではなく 00、01、10、11 を追加して、あらかじめ起きる衝突を回避することを意図したアルゴリズム上の工夫である。この aggressive advance は ID に偏りがあって衝突が連続して起きるような場合や、識別可能領域に存在するトランスポンダ数が多い場合に有効であるが、逆に偏りが少ない場合やト

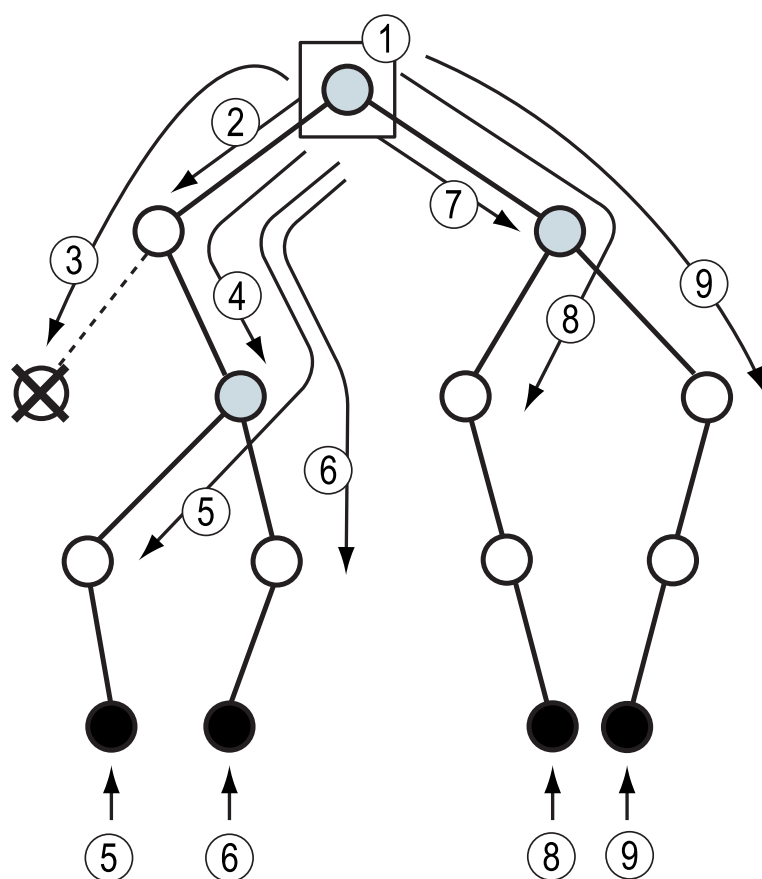


Figure 1.17: Query tree アルゴリズムの木構造

ランスポンダ数が少ない場合には余分な通信が増えてかえって効率を落してしまうので適用の際は注意する必要がある。

shortcutting 一方 shortcutting は、あらかじめ予測できる衝突を回避することによって認識時間を削減するための工夫である。たとえば、あるプレフィックスで衝突が起きたとして、そのプレフィックスに“0”を追加した場合に応答がなかったとすれば、“1”を追加しただけでは衝突が再び起こるのは自明である。そこで shortcutting ではこのような場合に 10 と 11 をそれぞれ追加して応答要求する。shortcutting は aggressive advance と異なり、どのような場合でも QT の識別速度に対する改善に効果がある。

指令	#1	#2	#3	#4	受信応答
REQ, ϵ	0101	0110	1011	1100	CCCC
REQ, 0	0101	0110	N/A	N/A	01CC
REQ, 00	N/A	N/A	N/A	N/A	Z
REQ, 01	0101	0110	N/A	N/A	01CC
REQ, 010	0101	N/A	N/A	N/A	0101
REQ, 011	N/A	0110	N/A	N/A	0110
REQ, 1	N/A	N/A	1011	1100	1CCC
REQ, 10	N/A	N/A	1011	N/A	1011
REQ, 11	N/A	N/A	N/A	1100	1100

Figure 1.18: Query tree の認識フロー例

Query Tree short long Query Tree short long (QT-sl) は QT におけるトランスポンダが応答するための通信量を削減することによって識別速度の向上を狙うアルゴリズムである [62]。QT-sl においてリーダーは 2 種類の応答要求指令を与えられる。すなわち REQ-short と REQ-long である。REQ-short 指令が送られるとプレフィックスに合致するトランスポンダは “1” を応答する。合致しないものは応答しない。このとき複数のトランスポンダが “1” を応答したということはリーダーで検出できなければならない。もし “1” を応答したものが複数存在すれば、プレフィックスの末尾に追加して再度 REQ-short を発行する。一方、応答したものが一つであれば、同じプレフィックスで REQ-long を発行し、絞り込まれたトランスポンダに全 ID データの応答を要求する。衝突により無駄になる応答が大幅に削減可能であるので、QT の速度向上に大きく寄与するアルゴリズムではあるが、複数が 1 を応答したということを検知するため、符号化や変復調方式において何らかの機構が必要である。

Query Tree incremental matching 木を下る段階ではプレフィックスの末尾以外は変化しないにもかかわらず、毎回これをリーダーが送信するのは通信時間の無駄である。この無駄を削減するためのアルゴリズムが Query Tree incremental matching (QT-im) である [62]。この手法は、QT におけるプレフィックス送信を増分のみとし、トランスポンダはその都度、増分をカウンタの示すビット位置と比較して状態遷移することで実現される。リーダーには QT-sl の REQ-short、REQ-long に加えて REQ-reactivate 指令が定義されている。トランスポンダはリーダーから送られてくる REQ 指令に応じてカウンタの示す ID ビットと逐次比較を行い、一致していれば “1” を応答する。一致していなければ transient 状態に移行する。transient

指令	#1		#2		#3		#4		受信応答
	応答	乱数	応答	乱数	応答	乱数	応答	乱数	
PARAM, $\lambda = 2$	—	1	—	0	—	1	—	1	Z
RESULT, 0	N/A	1	0110	0	N/A	1	N/A	1	0110
RESULT, 1	0101	1	N/A	0	1011	1	1100	1	CCCC
PARAM, $\lambda = 4$	—	2	—	0	—	3	—	0	Z
RESULT, 0	N/A	2	0110	0	N/A	3	1100	0	CCCC
RESULT, 1	N/A	2	N/A	0	N/A	3	N/A	0	Z
RESULT, 2	0101	2	N/A	0	N/A	3	N/A	0	0101
RESULT, 3	N/A	2	N/A	0	1011	3	N/A	0	1011

以下省略

Figure 1.19: Hashed query による認識フロー例

に移行したトランスポンダはその次の指令が REQ-reactivate でない限り inactive 状態に遷移する。transient 状態は、存在しないプレフィックスを要求してしまったときでもリーダーが探索を継続するためにある。この改良アルゴリズムによって、リーダーの指令・トランスポンダの応答ともに無駄を省くことができる一方で、トランスポンダに状態遷移のためのロジックが新たに必要となるので得失を考慮して導入する必要がある。

Hashed Query QT から派生したものに Hashed query (HQ) がある [68, 69]。HQ ではリーダーの問い合わせに応じトランスポンダが応答するのに変わらないが、問い合わせの対象として用いられるのが ID データではなくあらかじめトランスポンダに求めさせたランダム値であるということに相違点がある。HQ においては、リーダーの指令として PARAM, λ と RESULT, n が定義されている。PARAM 指令はトランスポンダに λ に満たない乱数を生成させる指令である。一方、RESULT 指令は生成した乱数値が n であるトランスポンダの応答を促す指令である。リーダーにとってトランスポンダの総数は未知であるから、これを確率的に導出することで適応的に衝突を回避する。

トランスポンダ群 N とリーダーとの HQ による通信例を Figure 1.19 に示す。はじめにリーダーは総数がわからないので $\lambda = 2$ として乱数生成する。偶然、“0” となったトランスポンダが一つしかなく識別することができるが、逆に“1” となったトランスポンダが三つ存在して衝突している。このため、リーダーは $\lambda = 4$ と調整して再び値の問い合わせを行う。これを繰り返して全てのトランスポンダが識別される。

1.4.1.5 Bin-slotted Hybrid Search

後述する s-ALOHA と bin tree アルゴリズムを組み合わせた手法として、Bin-slotted Hybrid Search (BHS) が提案されている [70]。この bin tree アルゴリズムは決定的手法における Binary Tree 法がビットごとに ID を分類して木構造を形成するのに対して、bin という単位を定義して bin ごとに木構造を形成する手法である。BHS-static では bin のサイズを 8 個に固定しており、また BHS-dynamic では 8 個から 64 個の間で可変になっている。いずれにしても、この 8 個以上ある bin にトランスポンダを分け、 m 分木としてトラバースすることにより衝突を回避する。このとき m は $8 \leq m \leq 64$ である。ここで、BHS の名前に含まれる hybrid という単語の意図するところは、bin を TDMA スロットに見立てて s-ALOHA に則りトランスポンダに bin ごとに一括応答させるので、決定的と確率的の双方の特徴を持つ手法であることを主張することにある。

BHS におけるリーダは PingID PTR, LEN, VAL, ScrollID PTR, LEN, VAL と Quiet PTR, LEN, VAL の各指令を行使することができる。まず、リーダは PingID 指令によって ID のどの部分を bin に割り当てるかトランスポンダに指示する。これにしたがってトランスポンダは指定部分の ID 値に対応した bin スロットに応答する。このとき、ID 値を送るのではなく QT-sl による REQ-short と同様、存在することだけを応答する。このとき衝突が起これなければ、ID 値を ScrollID 指令で取得する。次いで Quiet 指令によって取得済のトランスポンダによる応答を停止させる。衝突した場合は最初の衝突位置からの ID ビットを bin に割り当てさせる。これを繰り返して衝突を解決する。

ID 群 $N_2 \in \{001101000, 011111010, 011111110, 110100110\}$ について、BHS による識別手順を Figure 1.20 に示す。まず最初の 3 bit を用いてトランスポンダを bin に割り当てる。たとえば、トランスポンダ #1 の 001101000 であれば、001 番の bin スロットを用いて応答する (Figure 1.20(1))。ここで、#1 と #4 は衝突することなしに応答できるが、#2 および #3 はともに 011 番の bin に割り当てられるため応答が衝突する。続いて、衝突しなかったものについて ScrollID および QuietID 指令によって ID の取得と応答停止が行われる。衝突を回避できたトランスポンダの ID を全て取得したら、衝突したものについて処理をはじめめる。この場合、#2 と #3 は最初の 6 bit が一致しているので、7 bit 目からの 3 bit で bin に割り当てる。このとき、衝突した #2 と #3 のみ処理するために最初の 6 bit、"011111" を VAL に指定して PingID 指令を発行する。この

指令	TDMA スロット (bin)								
	000	001	010	011	100	101	110	111	
PingID, 0, 0, 0		#1		#2, #3			#4		(1)
ScrollID, 0, 3, 001	Tag #1 ID (001101000)								
Quiet, 0, 3, 001	Tag #1 → sleep								
ScrollID, 0, 3, 110	Tag #4 ID (110100110)								
Quiet, 0, 3, 110	Tag #4 → sleep								
PingID, 6, 3, 011111			#2				#3		(2)
ScrollID, 6, 3, 010	Tag #2 ID (011111010)								
Quiet, 6, 3, 010	Tag #2 → sleep								
									以下省略

Figure 1.20: Bin-slotted hybrid search による認識フロー例

結果、#2 は 011111010、#3 は 011111110 である (Figure 1.20(2)) から衝突が回避され認識が完了する。

1.4.2 確率的手法による衝突防止

全トランスポンダの識別を保証できる決定的手法とは異なり、識別できないトランスポンダの存在確率を 0 にすることができないアルゴリズムを確率的手法という。確率的手法に基づいた RFID では完全な識別を放棄する代わりに高速かつ高効率な識別処理を与えることができる。一般的にはリーダが個々の ID を問い合わせるようなことはせず、トランスポンダが個々に内蔵する乱数生成器を用いて通信に用いるチャネル番号をランダムに求め、トランスポンダが一括して同時応答することで達成される。認識結果に高度な信頼性を要求される応用には向かないが、高速で高い効率にて個体識別をする必要がある、物流や流通・販売などの分野で有用である。本節では ALOHA 手順と FTDMA⁶について解説する。

1.4.2.1 ALOHA 手順

無線伝送による多重ランダムアクセスを可能とする方法として 1972 年、ハワイ大学の ALOHA プロジェクトによって開発された手法に ALOHA 手順と呼ばれるものがある。施設が分散しているハワイ大学ではコンピュータのネットワーク化を実現するにあたりパケット無線を用いることとなったが、その際にコンピュータ間の無線伝送において、複数が同じ通信チャ

⁶Frequency and Time Division Multiple Access

ネルを使用しても通信内容が失われないように考え出された手続きである。最も古くから使われている無線パケット伝送のための輻輳制御方式であり、確率的手法に基づいた RFID でも広く用いられている技術であるため、まずハワイ大学で開発・使用された Pure ALOHA について説明し、続いてその派生として Slotted ALOHA および Framed ALOHA について解説を行う。

Pure ALOHA のコンセプトは非常に単純である。

- 送信側は任意のタイミングでパケットを送信する
- パケットが衝突することなく正常に受信できれば、受信側で ACK⁷ と呼ばれる受信確認パケットを伝送する
- 送信側はパケットを送信してから一定時間内に ACK が得られなければ、ランダムな時間後に再送する

パケットが衝突すると ACK が得られないので送信側によって再送される。また、ACK が他のパケットと衝突した場合も再送の対象となる。Pure ALOHA では全くランダムなタイミングで送信および再送するので、送受信双方においてタイミング同期をとる必要がない。一方で、送信側の増大に伴って衝突確率が飛躍的に増加する。これは同期を行っていないために、ある送信者がパケット伝送中に、その終了を待たずにほかの送信者が伝送をはじめてしまうことにより起こる。このようにパケットが一部でも衝突すると、送信者は伝送パケットを再送しなければならないために、通信の効率は送信者数に比例して低下する。

Slotted ALOHA Pure ALOHA に対して送受信双方が TDMA によるスロット同期を行った方式を Slotted ALOHA (s-ALOHA) という。この方式では、送受信間においてスロットと呼ばれる TDMA チャンネルを用いる [71]。ここで、送信者は任意のスロットにパケット送信し、再送もスロットに同期して行われる。このとき、送信後の一定期間内に受信側から ACK が返ってこなければ、送信者は衝突したとみなして再びランダムなスロットを選び、再送する。しかしながら、受信側はパケットがスロットに同期して送られることは知っていてもそれがいつ送られるかわからないため、通信期間を定義することができない。

⁷Acknowledgement (肯定応答)

Framed ALOHA Slotted ALOHA に対して送受信双方がさらにフレームという一定の通信期間を定める方式を Framed ALOHA という [72–75]。フレームは TDMA チャンネルである複数のスロットに分割され送受信に利用される。ここで、送信者は s-ALOHA と同じく任意のスロットにパケットを送信する。ただし、s-ALOHA とは異なり再送はフレーム単位で行われる。すなわち、送信側は次のフレームが始まるまでに受信側からの ACK を受信できなかった場合に限り、次のフレームでランダムにスロットを選んだ後にパケットを再送する [76]。送受信双方で同期をとることは、特にリーダが電力供給波をトランスポンダにブロードキャストする RFID ではさほど難しいことではないため、確率的手法に基づいた RFID は通常この Framed ALOHA に基づいて衝突を防止する。

Dynamic Framed ALOHA Framed ALOHA においてフレーム長は一定であった。このことは、送信者数が変化しない限り Framed ALOHA が有効に作用することを意味する。一方で、送信者数が時々刻々と変動、特に増加するような状況では、フレーム内で輻輳の解決ができずにスループットが劣化する問題がある。Dynamic Framed ALOHA では、この問題を解決するためにフレーム長を可変とする [77–80]。この手法は、前のフレームの輻輳状況から要求されるフレーム長を確率的に推測して動的に変化させることで、送信者数に対してスロットが少ないことによって起きる衝突の常態化を避けることを可能とする。RFID ではフレーム長を電力供給波に載せることで Dynamic Framed ALOHA も比較的容易に実現できる。オランダの Phillips Semiconductor 社（現・NXP Semiconductor 社）が開発した I-CODE[81] も Dynamic Framed ALOHA から派生したアルゴリズムを用いている。

いずれにしても、ALOHA は TDMA を基盤とするアクセス制御方式であるため、他の多重化と併用することができる。そのため、上述した BHS や後述する FTDMA、また本論文で提案する TS-CDMA⁸においても ALOHA 手順の派生系が適用されている。ALOHA は多重通信の基礎として今日では幅広く応用されているが、そのチャンネル利用効率が非常に悪いため、そのまま衝突防止アルゴリズムとして用いると衝突による誤り率および同時識別数の大幅な向上が望めない。

⁸Time Slotting-Code Division Multiple Access

1.4.2.2 FTDMA

FTDMA はオーストラリアの Magellan Technology 社が開発した方式であり、ISO/IEC 18000-3 Mode 2 [82] に物流用途向けの RFID 仕様として採択されている。FTDMA とは Frequency and Time Division Multiple Access の略で、周波数と時間分割による多重化を併用することで多重数を稼ぐ方式である [83]。この方式におけるトランスポンダはランダムに FDMA チャネルと TDMA スロットを選ぶことができる。RFID における FDMA は副搬送波を用いて実現される。そのため、システムは主搬送波たる電力供給波から生成されたクロックを分周して複数の副搬送波を得る。この Magellan 社による FTDMA 方式はリーダーがランダムミュート指令を発行できる点が特徴的である。この指令は各トランスポンダがフレーム内に応答するかどうかを、トランスポンダが内蔵する乱数生成器によって決定させる。ミュートする確率を指令として与えることで、リーダーが輻輳状況によって適応的にチャネル数に応じて応答トランスポンダ数を調整することを可能としており、この機構が識別性能に大きく寄与していることが明らかにされている。FTDMA は FDMA と TDMA の組み合わせにより実現されるため、FDMA チャネルの総数と同じだけの狭帯域チャネルを占有する必要がある。このことは、同時識別数のさらなる向上を困難にするばかりか、電波法令に基づく送信出力の制約が通信距離を大きく制限することを意味する。よって、FTDMA による RFID のリーダーは主に電磁遮蔽を目的としてトンネル型で実現され、狭帯域出力が外部に漏れ出さない。それゆえ、識別範囲はトンネルの大きさと厳密に定められ、識別範囲を任意に広げることができない。

1.4.3 本研究の位置づけ

このように RFID システムの認識に関わる性能を向上すべく、衝突防止アルゴリズムについてこれまでに様々な研究がなされてきた。本研究は、これらの従来研究における誤り率や同時識別数といった性能指標をさらに向上させた RFID システムを研究対象とする。本研究における衝突防止アルゴリズムと従来手法との関係を Figure 1.21 に示す。決定的手法による衝突防止アルゴリズムは誤り率をゼロにすることができるものの、同時に識別可能なタグ数が低いため性能を劇的に向上することができない。一方で、確率的手法によるアルゴリズムでは ALOHA や I-CODE といった誤り率・同時識別数ともに低いものと、FTDMA のように両者が比較的優れ

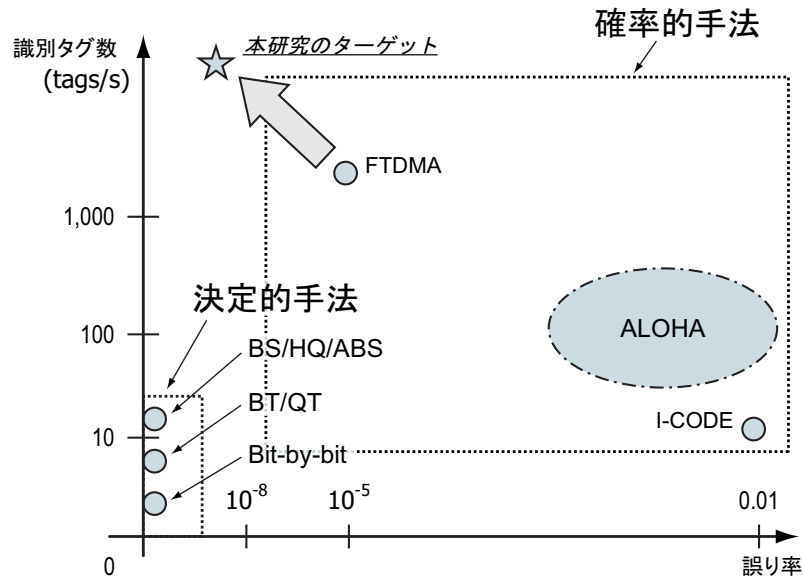


Figure 1.21: 各種の衝突防止アルゴリズムに対する本研究の位置づけ

ているものに二分される。本研究の対象とするRFIDシステムはこれまで研究されてきた多重RFIDシステム、特にFTDMAによるRFIDを超える性能を持つシステムである。これを本論文では超多重RFIDシステムと称する。

提案する超多重システムはFigure 1.21において、FTDMAよりも誤り率が低く同時識別数が多いことを示す、図の左上に位置する。その上で、本研究はトップダウンによる超多重RFIDシステムの設計手法を確立することを目的とする。その際、達成すべき目標としては超多重RFIDシステムの アナログ／デジタル (アナデジ) 双方の側面における設計・検証・評価手法を提案することである。目標に到達するためのアプローチとして以下の通り設定する。

- (1) 超多重RFIDの衝突防止アルゴリズムの考案
- (2) RFIDシステムの多重通信を対象とした設計および最適化手法の開発
- (3) アナデジ混載システムにおける統合的な検証ならびに評価手法の導出

1.5 研究の概要と本論文の構成

本節では研究の概要とともに各章の構成について説明する。2章では、超多重 RFID システムを実現するための衝突防止アルゴリズムを新たに提案（アプローチ (1)）し、これに基づく通信方式ならびに回路方式を明らかにする。3章では、高位モデル化手法としてハードウェア・エミュレータとソフトウェア・シミュレータの二者を用いて超多重 RFID 向け通信を実現するバックエンド回路の設計手法について提案（アプローチ (2)）する。4章では統合マルチレベルシミュレーション環境を新たに提案（アプローチ (3)）し、それを用いることによって可能となるアナデジ混載チップの設計手法について述べる。各章の概要について本節において説明する。

1.5.1 超多重 RFID システムの通信方式の提案

RFID はバーコードに変わる個別識別システムとして世界的に注目されている。RFID 市場が活性化する中、特に物流や流通分野においては識別の自動化やユーザの利便から導入がはじまりつつある。しかし、これらの分野では非常に大量の物品を扱う必要があるにも関わらず、これまで RFID の衝突防止アルゴリズムとして主に研究されてきた決定的手法では認識効率の改善が困難であった。この問題を解決するため、トランスポンダの一括応答を許容する確率的手法に基づく衝突防止アルゴリズムがいくつか提案されている。これらのアルゴリズムによって、トランスポンダの自発的な一括応答の実現により、認識効率を大幅に改善することができる。一方、市場の拡大に伴って今まで以上に識別効率の向上が求められている。そこで、2章では物流や流通分野への適用を視野に入れ確率的手法を用いた RFID 向け衝突防止アルゴリズムとして、Code Division Multiple Access (CDMA) に基づく手法を新たに提案する。また、提案するアルゴリズムを達成するための通信方式ならびに回路方式の提案を行う。はじめに、物流・流通における応用に適した高い認識効率を達成するために超多重通信を実現する衝突防止アルゴリズムならびにそれに基づく RFID システムの通信方式を提案する。次に、提案する通信方式を実現するための回路方式について議論する。最後に基礎的な方式検証としてテストチップの試作による実験を行う。

1.5.2 高位モデル化によるバックエンド設計手法の提案

認識効率を大幅に改善するための通信手法の議論の結果、2章で導出される数理的な解析に基づく分析では、現実システムへの対処ができない。実際の実装を考えて、さらに多くの評価項目の分析が必要である。そこで、擬似的な実験システムによるシミュレーションおよびエミュレーションによる高位モデル化を行うことで現実的な状況に照らしたシステムの分析や評価を行う。特に多重通信はデジタル処理を行うバックエンド回路によって実現されるため、このバックエンドの設計方針はシステムの性能に大きく関わる。そこで、3章では高位モデル化手法に基づくシステムパラメータの最適化と、超多重通信におけるロバスト性の評価を目的とする。はじめに、ハードウェア・エミュレータによる多重通信の基礎的な評価系を提案する。次に、提案する評価系を用いて多重 RFID の通信における性能評価を行う。さらに、ソフトウェア・シミュレータによるロバスト性の評価系を提案し、最後に提案する評価系を用いて 1,000 を超える多重通信のロバスト性に関する評価を行うとともにデジタル多重処理における性能を考慮した最適パラメータを導出する。

1.5.3 統合シミュレーション環境によるアナデジ混載チップの設計手法の提案

RFID の通信システムは無線を用いて実現されるので、変復調や電磁伝搬などアナログ領域に介在する外乱の影響を詳細に分析する必要がある。3章で提案する高位モデル化手法はエミュレータ、シミュレータいずれにおいてもデジタル領域の分析技術であり、外乱などの通信劣化をアナログ領域で評価できない。そこで、4章ではアナログ／ミックスシグナル・シミュレーションモデルとカスタムソフトウェアによる高位モデルの統合と、それにより可能となる超多重 RFID の外乱成分に対するシステム性能の評価を目的とする。はじめに、3章で提案するソフトウェア・シミュレータをアナログ／ミックスシグナルシミュレータに組み込むことで、アナデジ混載シミュレーションを可能にする統合マルチレベルシミュレーション環境を提案する。次に、この統合シミュレーション環境の特徴を明らかにするため、3章で提案する高位モデル化シミュレータとの比較を行う。この統合環境を用いて、2章で提案する超多重 RFID 向け通信方式をシステムレベルでプロトタイプ実装し、ノイズや電力変動などの外乱によるシステムの性能への影響を分析する。

第2章

超多重RFIDシステムの通信方式の提案

2.1 緒言

バーコードの置き換えとして注目されているRFID¹システムについて、その応用分野を広げるために認識効率の向上が課題となっている。特に、物流や流通、販売業務においては非常に大量の物品を扱う必要があるにも関わらず、これまで衝突防止アルゴリズムとして主に研究されてきた決定的手法は完全な識別に固執するあまり認識効率の改善が困難であった。この手法に基づくアルゴリズムでは全てのトランスポンダにリーダーが問い合わせる必要があるため、1秒に達成できる認識率は高々100個までであった。この問題を解決し識別効率を向上するためには、リーダーによる個々への問い合わせを完全に排除してとにかく速く応答させる必要がある。そのため、トランスポンダの一括応答を許容する確率的手法に基づく衝突防止アルゴリズムがいくつか提案されている。たとえば、Framed ALOHA や、Dynamic Framed ALOHA、FTDMA があげられる。トランスポンダの自発的な一括応答を実現することによって、確率的手法は認識効率を大幅に改善する。これらの手法により1秒間に最大で600個前後の認識ができるようになったが、それでもなおアパレルなどの流通分野における応用を考慮すると、これらの手法でも十分とは言えず、さらなる識別効率の向上が求められている。すなわち、これまで実現されてきた確率的衝突防止技術は、主とする多重化技術がTDMA²またはFDMA³であるためノイズへのロバスト性やチャネル容量が低く、それゆえ認識効率をさらに向上させることが困難である。そこで、本章では物流や流通分野への適用を視野に入れ確率的手法による認識効率の非常に高いRFID

¹Radio Frequency Identification

²Time Division Multiple Access

³Frequency Division Multiple Access

向け衝突防止アルゴリズムとして CDMA⁴に基づく手法を新たに提案する。また、提案するアルゴリズムを達成するための通信方式ならびに回路方式の提案する。はじめに、物流・流通への応用に適した高い認識効率を達成するために超多重通信を実現する衝突防止アルゴリズムならびにそれに基づく RFID システムの通信方式を提案する。次に、提案する通信方式を実現するための回路方式について議論する。最後に基礎的な方式検証としてテストチップの試作による実験を行う。

2.2 システムアーキテクチャ

通信方式の詳細仕様を説明する前に、本節において想定する応用例、前提とするパラメータについて説明する。

2.2.1 想定する応用例

提案する通信方式は物流ならびに流通の分野において業務の効率化を図ることを目標とする。具体的には、たくさんの商品が入った箱から梱包を解くことなく、何がどれだけ入っているかを一挙に把握できるようにする RFID システムの実現を目指す。応用例として Figure 2.1 に示されるようなシステムを考える。あらかじめ識別対象である商品や物品に識別用のタグを取りつけておく。タグにはトランスポンダが内蔵されており、無線伝送により識別される。それらが梱包された箱をそのままベルトコンベア上のゲートに通すと、トランスポンダがゲートに反応して識別情報を送信する。ゲートに設置されたリーダは、その情報を取得することで何が箱の中に入っているのかを診断することができる。この RFID システムは流通業における商品の入出荷処理や、物流業での物品の配送状況の管理、製造業での製品の仕分け、あるいは小売店舗での精算などの局面において利用されることを想定する。

物流業では特に秒速 2.5 m を超える高速なベルトコンベアが使われているため、通信方式の策定においてはその点も考慮にいれ、システムパラメータの設計を実施した。

⁴Code Division Multiple Access

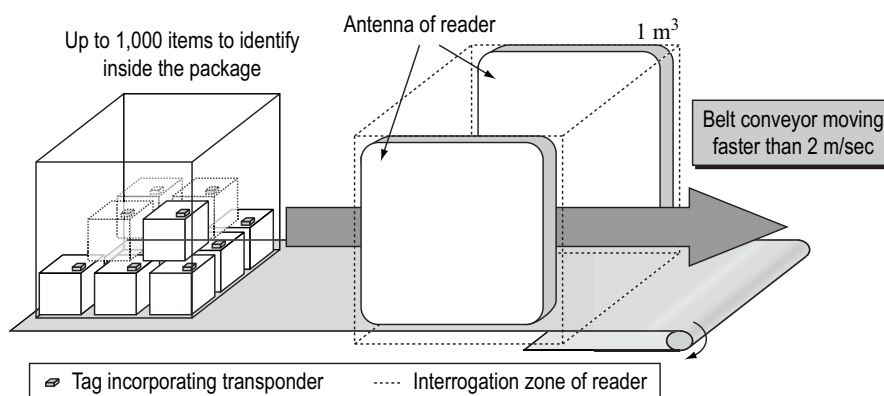


Figure 2.1: 超多重 RFID システムの応用例

2.2.2 システムパラメータ

2.2.2.1 ID ビット長

識別のため、タグには個別の ID 値が与えられる。この ID は全て異っており、一つとして同一の ID を持つタグは存在しない。タグは識別情報として自分の ID データを送信する。これを受信したリーダはどのタグが存在するか、すなわちそこにある品物は何であるのかということを認識する。

このとき、タグに持たせる ID ビット列の長さは識別可能な物品数に影響を与えるパラメータであるため、適切な長さにする必要がある。これは、短すぎると認識できる個体の種類が少なくなるので実用上の利便が損なわれる一方、長すぎると通信に必要な時間が長くなって認識効率が低下し、伝送中の通信チャンネルに介在するノイズによって引き起こされる誤りの発生率の増加が問題となる。

本提案システムは、流通分野への応用を視野に入れている。そのため、ID をあらゆるものに割り振ってもすぐに枯渇することがないだけの ID ビット長、すなわち 128 bit とする。これは 10^{38} 種類の物品識別を実現し、実用において必要十分な数量である。

2.2.2.2 最大同時識別数

最大同時識別数とは、識別のためのタグが同じ箱の中に最大どれだけ存在することを許容できるか、すなわち提案する通信方式による衝突防

止アルゴリズムが対応する最大の情報伝送数である。

これまで研究されてきた衝突防止アルゴリズムの中で最も効率が高いものは確率的手法によるISO/IEC 18000-3 Mode 2であり、879 msに500個の識別が可能である。一方、本研究では400 msに1,000個の物品識別を目標とする。この数量は一辺の長さが1 mの箱の中に一辺100 mmの物品、たとえば衣類や電子部品のような小物を詰めたときの個数に相当する。これにより、従来ではなし得なかった高速認識を実現し、RFIDの利用拡大を促す狙いがある。

2.2.2.3 最大応答時間とリーダアンテナ

想定するシステムではベルトコンベアに物品を梱包した箱を載せ、そのままゲートを通する間にゲートに設置されているリーダと物品に取り付けたタグの間でID情報の交換が完了しなければならない。リーダのアンテナ幅、すなわち識別可能領域を1 mとすると、秒速2.5 mを超える高速コンベア上での個体識別を可能とするためには $1/2.5 = 0.4$ s以内に全ての認識処理を終えなければならない。

ここで、コンベア速度を固定して考えると、識別領域を大きくすることによって情報交換に要する時間を長くとることができる。しかるに、領域を広げるとトランスポンダの微弱な応答波の到達範囲を超えてしまい、取得できないタグIDが発生する。また、トランスポンダへの電力供給がまばらになってリーダの受信処理に影響が起きる。これらのトレードオフを検討した結果、13.56 MHz帯におけるトランスポンダの応答範囲は1 m程度である[51]ことから、提案方式ではアンテナ幅を1 mに固定し、許容する最大応答時間を400 msとする。

2.2.3 電磁パラメータ

2.2.3.1 周波数帯域

日本国内における電波法にてRFID向けに割り当てられている周波数帯域として、135 kHz、13.56 MHz、2.45 GHz、5.8 GHzがある。

135 kHz帯は高出力化が可能であるため、通信距離を長くすることができる。一方、電磁誘導の性質が強く搬送波の波長が長いためにアンテナ長がボトルネックとなって小型化が難しいという欠点がある。また、トランスポンダの通信速度も律速される。ISO/IEC 18000-2に標準仕様が策定[84]されている。

13.56 MHz 帯は電磁結合と電波伝搬の中間的性質を持つ [82]。アンテナ長を短くすることができるので、小型化が容易である。また、2002 年 5 月に行われた法規制の緩和に伴って高出力化が可能となった。このため、最も扱いやすい帯域であり、利用者も多いため導入コストも低い。結合の性質によってノイズへのロバスト性が高く、水分による到達範囲への影響も少ない。

2.45 GHz 帯および 5.8 GHz 帯はマイクロ波であり、波長が短いのでアンテナを小さくすることができる。タグも小型化が容易で、直進性が高いため通信距離も比較的長くできる。一方、高周波であるために設計ならびに実装が難しいという欠点があり、製造コストも比較的高い。GHz 帯は高速に通信できるため、13.56 MHz 帯とともに現在注目をされている帯域である [85]。

そのほかに VHF/UHF として 433 MHz や 900 MHz 帯を用いる規格が策定 [74, 86] されている。

以上の特徴を検討し、非接触送電に有効な電磁結合の性質を持つこと、通信速度がさほど遅くないこと、アンテナ長を短くできること、実験するにあたって困難がつかまとう高周波ではないことを鑑みて、本研究では 13.56 MHz 帯を用いる。なお、提案する通信方式は周波数帯域と独立しているため、2.45 GHz 帯をはじめとする他の帯域への適用も可能である。

2.2.3.2 出力電波の強度

13.56 MHz 帯の電波出力は電波法令により Figure 2.2 に示すとおり規制される。具体的には、10 m における電界強度は $47544 \mu\text{V}/\text{m}$ 以下である。リーダの供給する電力供給波が制限されるため、トランスポンダの受電可能範囲は限定される。

一方、本方式においてタグの応答波はスペクトルの拡散に伴い帯域幅が広がり、Figure 2.2 に示す帯域を超える。そこで、トランスポンダの応答波は電波法で規定されるところの微弱波とする。すなわち、応答信号の電波出力は 10 m での電界強度が $150 \mu\text{V}/\text{m}$ 以下に制限され、トランスポンダの応答可能範囲も制限される。これらの制限を勘案すると、1 m の識別領域は妥当である。

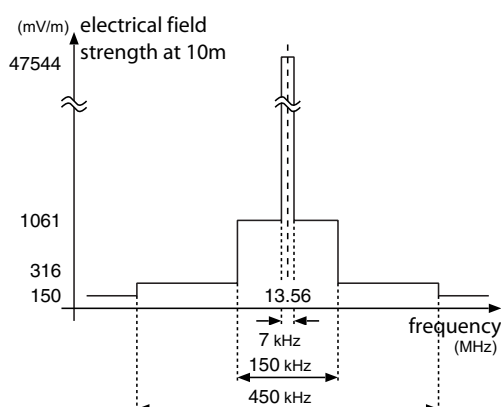


Figure 2.2: RFID 向け 13.56 MHz 帯の電界強度

2.3 超多重RFID向け通信方式

2.3.1 概要

RFIDシステムはトランスポンダとリーダから構成される。Figure 2.3にシステム全体のブロック図を示す。トランスポンダを内蔵しているタグは識別すべき個体に取り付けられ、リーダの応答範囲に入ると応答し始める。このとき、トランスポンダがID値を送信しはじめ、リーダがそれを受信することでシステムは個体を識別する。トランスポンダは自立した電源を持っておらず、リーダからの誘導結合により電力供給されて動作する。ID値はトランスポンダに内蔵されているROM⁵に記憶されており、多重化および変調された後にアンテナから送信される。一方、リーダは受信した信号を復調し、多重信号を分離したのちに誤り検出を行い正しいID値をデータベースに蓄積する。トランスポンダはそれぞれ固有のID値を保持しており、これにより個々の識別が可能となる。具体的には、リーダはID値を受信すると、それをIDデータベースを持つPC⁶に送り、リーダの応答範囲に存在する個体についての情報を得る。

提案されるリーダとトランスポンダ間の通信シーケンスをFigure 2.4に示す。概要は以下の通りである。

- (1) **リーダ**は識別可能領域に電力供給用の電磁波を連続的に送信する。

⁵Read-only Memory

⁶Personal Computer

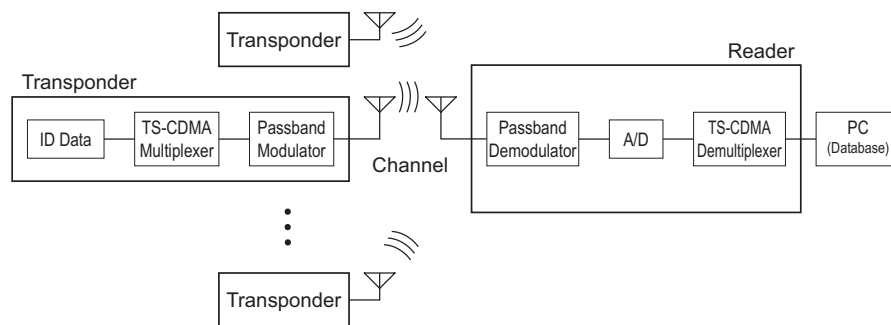


Figure 2.3: RFID システムの構成図

トランスポンダは識別領域に入ると内蔵するキャパシタに受信電力をチャージして通信回路の電源を投入する。

- (2) **リーダ**は電力波の位相を 180° 反転させてタイミングを知らせ、トランスポンダに同期を要求する。

各トランスポンダはリーダとの同期を取ってから内蔵ランダム生成機構を起動して通信チャンネルを選択する。

- (3) **トランスポンダ**は一括してROMに格納されたIDの送信を開始する。IDデータはスペクトル拡散と一次変調されてから、TS-CDMA⁷方式に則ってアンテナから輻射される。全IDビットの送信が終われば、トランスポンダは引き続きCRC⁸による誤り検出符号を送信する。

リーダは送信されたビット列を受信する。この受信信号は復調、デジタイズされたのちに逆拡散される。それからリーダのメモリに格納される。

- (4) **リーダ**はCRC符号をビット列から抽出してデータの正当性を確認する。正しいデータはコンピュータに転送され格納される。
- (5) 再送: 手順 (2)–(4) を繰り返す。

⁷Time Slotting-Code Division Multiple Access

⁸Cyclic Redundancy Check (巡回冗長検査)

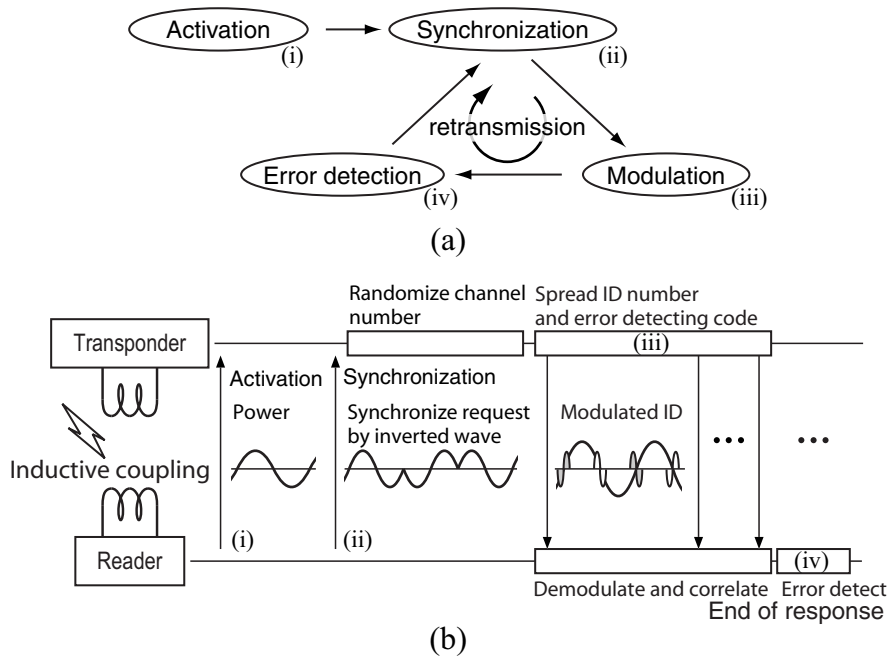


Figure 2.4: 超多重 RFID システムにおける通信の概要: (a) システムの状態遷移図、(b) 通信システムのシーケンス図

2.3.2 ダウンリンク

2.3.2.1 電力供給

パッシブ型のトランスポンダは独立電源を持たないので電力線や電池交換を排することができ、高い利便性を得ることができる。このトランスポンダが動作するために必要な電力はリーダから非接触給電により供給される。電力供給波はその周波数帯域により電磁結合か電波伝搬かの違いはあるものの、いずれにしてもトランスポンダがリーダから受け取る電力波は正弦波であり、その電圧成分は AC 電圧 [36] である。しかるに、デジタル回路は DC 電圧で動作するため、トランスポンダは供給された電力を整流する必要がある。整流としてはトランスポンダのアンテナであるバイファイラコイルを用いて全波整流を行う。この全波整流によって得られた DC 成分はトランスポンダ内の キャパシタ (コンデンサ) にチャージされ、回路の駆動に用いられる。したがって、キャパシタの容量はデジタル回路やタイミング抽出回路、ならびに変調回路すべてにかかる動作電力と ID データの送信に必要な電力をチャージするのに十分

な大きさのものを用意する必要がある。しかしながら、面積ならびに製造コスト上の制約によりキャパシタの容量はできるだけ低く抑える必要がある。このことは、トランスポンダの消費電力が厳しく制限されることを意味する。これらの背景により、低消費電力性を満たす通信方式および回路方式の導出が不可欠である。

2.3.2.2 同期

多重通信システムにおいては、トランスポンダとリーダーで同期を取ることが不可欠である。しかし、同期処理にはタイミング抽出やトラッキング制御といった負荷の高い演算が必要であり、大規模な回路を要求する。そこで、このような処理を排除するために同期パルスを用いる。電力供給波を適当なタイミングで1パルスの間、 180° 反転することにより双方の同期をとる手法により電力消費を抑えつつ、同期動作を実現する。

2.3.3 アップリンク

2.3.3.1 一次変調方式

多くの RFID システムでは、一次変復調方式として負荷変調による振幅変調 (Amplitude Shift Keying; ASK) を用いている。しかるに、負荷変調は送信動作中の全トランスポンダが内部のインピーダンスを各々変化させることになるので、インピーダンス整合が困難であり、電力を十分かつ均一に供給することができない。一般的なデジタルの一次変調方式として ASK のほかには、周波数変調 (Frequency Shift Keying; FSK)、位相変調 (Phase Shift Keying; PSK) などがあげられるが [87, 88]、これらの変調方式は、トランスポンダにオシレータを必要とするため消費電力を抑えることができない。そこで提案方式では、一次変復調として Ultra Wideband-Impulse Radio (UWB-IR) [89, 90]、すなわちインパルス変調を用いる。これにより消費電力を抑えつつ省スペースでトランスポンダ回路が実現可能である。

Figure 2.5 に変調波形を示す。点線で示されているのがリーダーからの電力供給波であり、実線がトランスポンダからの応答波である。変調はガウスモノサイクルパルスを輻射することによって行われる。輻射されたパルスはスペクトルが拡散するため小電力でも受信側で復調することができる。本研究では、インパルス列で“0”と“1”を表現するために Bi-phase Pulse Position (BP³) 変調を提案する。変調信号は電力供給波の干渉を避

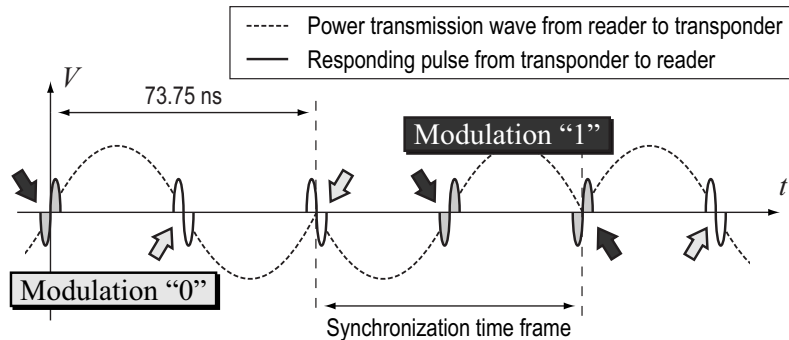


Figure 2.5: インパルスによる一次変調波形

けるために電力波がゼロと交差する近傍において輻射される。このとき、“0”は電力波が正から負へ遷移するときのゼロ付近で位相が 0° のモノサイクルを、また“1”は電力波が負から正へ遷移するときのゼロ付近で位相が 180° のモノサイクルを送出することによって表現される。

2.3.3.2 一括応答のための衝突防止機構

リーダの識別可能領域に複数のトランスポンダが存在するとき、全てのトランスポンダが同時に応答すると通信チャネル内での相互干渉によって識別情報が失われる。それゆえ多重通信を実現するためには衝突防止機構を欠かすことができない。そこでTS-CDMAによる衝突防止アルゴリズムを考案した。その詳細について以下で説明する。

DS-CDMA Direct Sequence-CDMA (DS-CDMA)は従来の多重通信方式、たとえばFDMAやTDMAと比較して多重信号間の相互干渉を低く抑え、かつスペクトル占有において高い効率を与えることができる[91, 92]。提案する通信方式はFigure 2.6に示す通りCDMAとTDMAを組み合わせ、消費電力ならびに実装面積を低減することができる。なお、要素技術であるFDMA、TDMAならびにCDMAについては付録Aに詳述する。

DS-CDMAでは通信チャネルは拡散符号によって区別される。数千個のトランスポンダが同時通信するためには、少なくともトランスポンダ数と同じだけのチャネルが必要であるから、トランスポンダに割り当てられて占有される個別の符号も数千種類必要とされる。このとき、リーダと応答するトランスポンダ間における符号の割り当て情報の交換には長い時間を要し、電力ならびに実装面積の増大につながる。そのため、チャ

ネル割り当てのための事前折衝は排除する。これはトランスポンダが拡散符号をランダムに選択することで実現できる。

DS-CDMA においては、拡散符号数を n 、トランスポンダ数を r とおくと、 $r \leq n$ を満たさなければならない。一般的には、 n 種類の符号からランダムに r 個を選び出したとき、複数のトランスポンダが同じ符号を選んでしまう確率、すなわち衝突確率は

$$\begin{aligned} P_r(\xi, n, r) &= \left(1 - \frac{\xi C_n}{\xi H_n}\right) \cdot \left(1 - \frac{n C_r}{n H_r}\right) \\ &= \left(1 - \frac{\xi C_n}{\xi + n - 1 C_n}\right) \cdot \left(1 - \frac{n C_r}{n + r - 1 C_r}\right) \end{aligned} \quad (2.1)$$

と表される。ここで、トランスポンダ数を ξ とし、 $n C_r$ は n から r を選びだすときの組合せの数、また、 $n H_r$ は n から r を重複を許して選びだすときの組合せの数を表す。

たとえば、トランスポンダ数 r が 1,024 のとき符号数 n が 1.00×10^7 よりも大きければ衝突確率 P_r は 0.1 以下となる。したがって、ランダムに符号選択しても低い衝突確率となる 1,000 の CDMA 多重を実現するには単純に見積もって 1,000 万種以上の拡散符号が必要である。CDMA 方式ではそれぞれの拡散符号が直交性を持たなければならないので、直交性のないものよりも個々の符号を長くせざるを得ない。具体的には、CDMA 方式のみで 1,000 トランスポンダを同時に識別する性能を達成するためには、10 Mbit を超える拡散符号を使用する必要がある。

一方で、トランスポンダの応答が周波数 $f_{\text{tr,ck}} = 13.56$ MHz、すなわち周期 $T_{\text{tr,r}} = 1/f_{\text{tr,ck}} = 73.7$ ns によって行われるとすれば、トランスポンダが $t = 400$ ms 以内に応答することができる最大の拡散符号長は

$$\frac{t}{T_{\text{tr,r}} \cdot l_i} = \frac{400 \times 10^{-3}}{73.7 \times 10^{-9} \times 128} = 4.24 \times 10^4$$

と表される。すなわち、目標とする通信時間を達成するための拡散符号は 42 kbit に制約される。10 Mbit の拡散符号では目標の通信時間を満たせないばかりか、トランスポンダに内蔵される拡散符号の生成回路の面積や消費電力も非常に大きくなり、CDMA だけで実現することは現実的に不可能である。

TS-CDMA 本方式では通信方式として、DS-CDMA にかえて Time Slotting-Code Division Multiple Access (TS-CDMA) により数千個のトランスポ

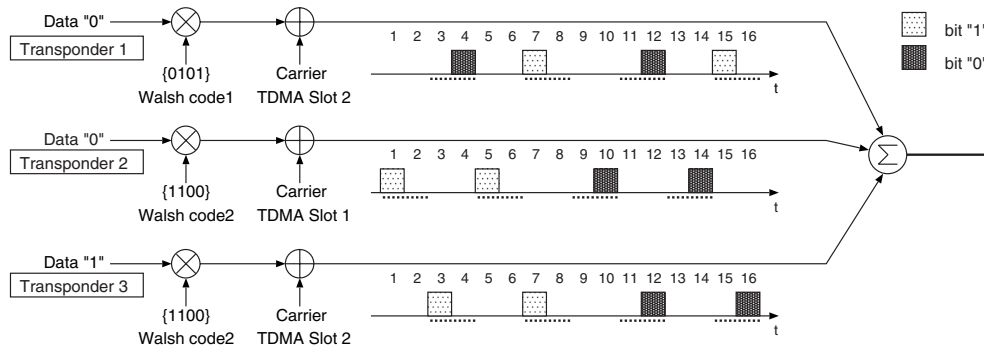


Figure 2.6: TS-CDMA 方式による多重化の概念

ンダの同時識別を実現する。TS-CDMA は、DS-CDMA と TDMA を組み合わせた通信方式であり、少ない拡散符号で 1,000 多重を実現でき、かつ回路規模を最小化できる。トランスポンダとリーダは一次変復調回路と同様、個々に TS-CDMA 変復調回路を持つ。

TS-CDMA 方式に基づく多重化について Figure 2.6 によって説明する。このとき、トランスポンダ数を 3、拡散符号長を 4、またスロット数を 2 とする。図は各トランスポンダが 1 bit の ID を多重化して出力したときの様子を表す。多重化プロセスは、まず ID と拡散符号の各ビットとの排他的論理和 (eXclusive OR; XOR) を取ることから始まる。この XOR 演算によって ID ビットの拡散を行う。Figure 2.6では拡散符号長が 4 bit であるので、1 bit の情報が 4 bit に拡散される。次に、この拡散信号をあらかじめ選択したスロットにて送信する。ビット情報は一次変調においてモノサイクルパルスの位相差とその送信タイミングで表現するため、Figure 2.6ではスロットを 2 周期に拡大して表す。すなわち、 $t = 1, 2$ のときスロット 1 である。また、 t が奇数のときが “1”、偶数のときが “0” の変調タイミングとして図示されている。選択したスロットに対してビット値でタイミングを変えながら、拡散信号を一次変調して送信する。各トランスポンダの出力は通信チャネルにおいて足し合わされ、リーダシステムに到達する。

リーダがトランスポンダごとに異なる通信チャネルを決定し、各トランスポンダに通知していた従来の決定的手法と異なり、本方式では事前折衝を行わない。トランスポンダは疑似乱数系列生成回路 (Pseudo Random Sequence Generator; PRSG) を用いて、1,000 以上の通信チャネルから一つを自発的に選択し使用する。この手法は、s-ALOHA を適用した DS-

CDMA と同等である。この PRSG によるスロット選択によって通信処理を簡単化し、トランスポンダの消費電力を低減することができる。TS-CDMA において一連の拡散／逆拡散手続はデジタル信号処理により実装される。

TS-CDMA において、複数のトランスポンダが単一の拡散符号を共有する確率は次のように表される。

$$\begin{aligned} P_c(n, r, \xi, x) &= P_r(\xi, n, r) \cdot P_t(\xi, x) \\ &= \left(1 - \frac{\xi C_n}{\xi + n - 1 C_n}\right) \cdot \left(1 - \frac{n C_r}{n + r - 1 C_r}\right) \\ &\quad \cdot \left(1 - \frac{\xi C_x}{\xi + x - 1 C_x}\right), \end{aligned} \quad (2.2)$$

ここで、スロットの選択に伴う衝突確率は $P_t(\xi, x)$ と表されており、トランスポンダ数を ξ 、スロット数を x とする。式 (2.2) は $P_r(\xi, n, r)$ または $P_t(\xi, x)$ が 1 に近いとき、すなわち r の n に対する比率または x の ξ に対する比率が十分に小さくないときを除いて TS-CDMA の衝突確率は DS-CDMA や TDMA 単体のものよりも低いことを示す。たとえば、 $P_r(\xi, n, r)$ は符号数 n を 1,024 とおいたとき、通信チャネル数 r が 64 より大きくなると 1 に漸近する。Table 2.1 に衝突確率に関するパラメータの比較を示す。CDMA のみの場合と TDMA のみの場合では衝突確率を低くするためには CDMA においては拡散符号数を、また TDMA においてはスロット数を極めて大きくしなければならないので、他と較べて長い通信時間が必要となることが示されている。ここで、TS-CDMA による通信パラメータの最適な組み合わせは注意深く導出されなければならない。システム要求に応じたパラメータの候補を導出し、Table 2.1 に示す。この導出結果より、提案する手法は十分に低い誤り率でシステム要求を実現できることを見出した。

2.3.4 通信制御

2.3.4.1 再送

無線伝送システムにおいて考慮しなければならない事項の一つとして、通信誤りへの対処がある。何らかの理由で電波伝搬状況が悪化して通信中のデータにノイズが重畳すると、正しい信号が受信できない。

本通信方式では、通信制御をできる限り簡素化することで回路面積ならびに消費電力の削減を図っている。そのため、リーダーからトランスポ

Table 2.1: 理論的な導出による RFID システムパラメータの比較

	full CDMA	TD-CDMA		full TDMA
ξ : # of transponder	—	1024	1024	10.0M
n : # of Spread code	10.0M	16	16	—
r : # of CDMA ch.	1024	2	4	1
x : # of TDMA ch.	1	512	256	1024
t_{TX} : Time frame [ms]	106000	87.0	43.5	106000
τ_{TX} : Max. time frame [ms]	400	400	400	400
κ : Max. # of allowable re-transmission	0.004	4.60	9.20	0.004
l_i : Length of ID	128	128	128	128
l_c : Length of CRC	16	16	16	16
P_c : Collision probability	0.095	2.46×10^{-2}	0.111	0.095
P : ID error rate	—	3.65×10^{-7}	2.52×10^{-9}	—

ンダに送られる信号は電力供給のための正弦波と、それに埋め込まれた同期信号のみであり、トランスポンダに対して明示的に拡散符号やスロットを割り当てることはない。言い換えるとトランスポンダは自発的、つまりランダムに使用する拡散符号およびスロットを決定する必要がある。このとき、たとえ式 (2.2) で与えられる衝突確率 $P_c(n, r, \xi, x)$ が 0.01 に満たなくとも、依然として複数のトランスポンダが同一の拡散符号、同一のスロットを選択する可能性はゼロではない。これは、拡散符号とスロットが共有されて衝突が起きることにより、トランスポンダの応答は混ざり合って失われるためである。そのため、ノイズの影響で誤りが発生してもデータを取得できること、また衝突が起きる確率をできるだけ小さくすることを鑑みて、トランスポンダは電力が供給されている間、常に同期して ID データの再送を繰り返す手法を採った。

2.3.4.2 ランダムスロットシフト方式

再送の際に用いる拡散符号や送信スロットが常に同じであるならば、何度再送を繰り返しても衝突を免れることはできない。これを防ぐため、再送のたびにトランスポンダは通信スロットをランダムに選びなおす。最終的にリーダは低い衝突確率で ID データを受信することができるのである。このとき、ID の送信が少なくとも k 回行われ、毎回の通信試行において拡散符号とスロットが変化するとすれば、衝突確率は

$$P(n, r, x, k) \leq P_c(n, r, \xi, x)^k \quad (2.3)$$

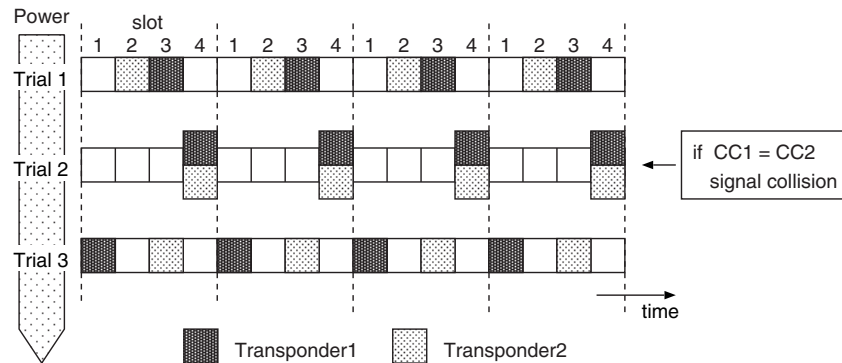


Figure 2.7: ランダムスロットシフト方式のシーケンス例

である。

TS-CDMA と再送制御を用いた信号の送信例を Figure 2.7 に示す。ここでは、トランスポンダ数を 2、ID ビット長を 1、拡散符号長を 4、スロット数を 4 として、3 回送信する間は電力供給が続くとする。各トランスポンダは再送ごとにスロットと拡散符号をランダムに選択して送信するが、ここで選択したスロットが重複する場合でも異なる拡散符号を用いていれば信号の分離が可能である。一方、同一の拡散符号を用いていれば、信号が衝突する。しかし、それ以外の再送で一度でも信号が正しく分離できれば、トランスポンダの信号はリーダーに正しく伝送されたことになる。以上のように、本方式では再送制御によってシステムの信頼性を向上している。s-ALOHA⁹ 手順と較べると、提案する手法は正常に認識できたトランスポンダも応答を続けるため、衝突回避プロセスが非効率である。しかしながら、トランスポンダに同期パルス以外の受信機能を持たせる必要がなく、回路面積および消費電力を削減することができる。また、s-ALOHA と同様に認識できたトランスポンダによる応答を肯定応答 (Acknowledgement; ACK) 信号によって停止させれば、ID 誤り率は向上することが期待できるが、その分の回路面積、消費電力は増大する。

一方で、再送がなくとも TS-CDMA 方式は CDMA による多重化も行われているため、スロットが共有されても拡散に用いられた符号が異なれば分離可能である。ここでも、TS-CDMA 方式は CDMA の実現による回路規模、消費電力や通信時間のオーバーヘッドを TDMA の併用によって最小限に抑えつつ、TDMA に較べてスペクトル拡散に伴うノイズなど

⁹Slotted ALOHA

外乱へのロバスト性や通信内容の信頼性を高めることが可能である。

2.3.5 誤り検出

無線伝送のようにノイズの影響が無視できない通信チャネルにおいて、確実にデータ通信を行うためには誤りが発生したことを検出する必要がある。そのためにデータの一部に冗長な検査用のデータを付加する方法が広く行われている。リーダは通信誤りを認識して不正な ID データを破棄するために誤り検出符号を用いる。誤り検出システムは送信の際にデータに冗長な符号を付加するエンコーダと、受信した冗長符号を評価して受信データの正当性を確かめるデコーダから構成される。誤りを検出すると、受信した ID データは単純に破棄される。このことは、受信側にあるデコーダは受信データの誤りを訂正しないことを意味する。すなわち、誤った受信データの回復は再送によってのみ達成される。

現在では、誤り検出あるいは訂正が可能な方法として様々な誤り検出符号が提案されている。この誤り検出符号は大きく分けてブロック符号と畳込み符号に分類される。ブロック符号としてはパリティ符号、水平冗長検査 (Longitudinal Redundancy Check; LRC) 符号、巡回冗長検査 (Cyclic Redundancy Check; CRC) 符号が、また畳込み符号としては Turbo 符号、Reed Solomon (RS) 符号、低密度パリティ検査 (Low Density Parity Checking; LDPC) 符号があげられる。ブロック毎に符号の生成を行うブロック符号に比べ、前のブロックの符号化が次のブロックの符号に影響する畳込み符号は誤りを訂正する能力が高い [93] が、符号化のみならず検査側にも多大な演算能力を要求する [94]。

確率的 RFID システムでは、通信誤りが発生する局面が2つあげられる。(1) 通信チャネルを伝搬する過程において混入するノイズによる影響と、(2) 多重化の過程で偶然、拡散符号とスロットが一致して発生するゴースト ID による影響である。これらの誤りに確実に対処するためには、ブロック毎に誤りの有無を確定できるブロック符号の方が、確率的な復号アプローチをとらざるを得ない畳込み符号よりも望ましい。また、トランスポンダ側の回路規模や消費電力を鑑みても符号化にかかる演算量が比較的少ないブロック符号が適切である。

提案システムではエンコーダがハードウェアで容易に実現できて、信頼性の高いチェックサムを提供することができるという理由で CRC 符号を用いる。

2.3.5.1 検出能力

二種類の誤りが発生する局面のそれぞれにおける CRC 符号の検出能力について分析する。

ノイズによる誤り CRC 符号の検出能力は符号長が $2^n - 1$ を超えない場合、

- $n = 16$ のとき 3 個まで、 $n = 32$ のとき 11 個までの誤り
- 奇数個の誤り
- 長さ n までのバースト誤り
- 長さ 2 までの二重バースト誤り

を検出することができる。またバースト誤りの長さが n を超えても高い確率で検出が可能である。

ゴースト ID による誤り 異なる ID を持つタグが、同時に同じ拡散符号で同じスロットを利用して通信を始めたとする。このとき、 n bit の CRC で誤りが検出できない確率は、混合により得られたゴースト ID から求めた n bit の CRC 符号が混合して与えられた CRC 符号と偶然に一致する確率である。これは $P_e = 2^{-n}$ で与えられる。したがってゴースト ID による誤りに対する CRC 符号の見逃し率は、16 bit の CRC 符号の場合で $2^{-16} = 1.526 \times 10^{-5}$ 、32 bit の場合 $2^{-32} = 2.328 \times 10^{-10}$ である。

以上の分析から CRC 符号の導入による検出能力の改善程度を明らかにした。しかるに、符号長の増加はエンコーダの面積、消費電力、ならびに通信時間に影響する。ここで、CRC 符号を用いても誤りを検出できない確率 P_n は CRC 符号長が 16 bit の場合

$$2^{-16} \cdot P_c(n, r, \xi, x) = 1.526 \times 10^{-5} \cdot P_r(\xi, n, r) \cdot P_t(\xi, x)$$

に等しい。この確率値は $P_c(n, r, \xi, x) \leq 0.1$ とおいたとしても 10^{-6} に満たない。誤り率と符号の伝送にかかる時間の間にあるトレードオフを考慮すると、16 bit の CRC 符号がシステムに敵しているといえる。よって誤り検出システムとして 16 bit の CRC 符号を採用した。なお、生成多項式は ITU-T¹⁰ 勧告による $x^{16} + x^{12} + x^5 + 1$ とする。

¹⁰ International Telecommunication Union (ITU) Telecommunication Standardization Sector, 1993 年に Comité Consultatif International Téléphonique et Télégraphique (CCITT) から改組。

2.3.6 通信時間

全トランスポンダが TS-CDMA 方式によって ID データを送信するのにかかる一回あたりの時間 T_{TX} は、ID 長を l_i 、CRC 長を l_c 、拡散符号長を n 、TDMA スロット数を x とおくと、

$$T_{\text{TX}} = \frac{1}{13.56 \times 10^6 \text{ Hz}} \cdot (l_i + l_c) \cdot n \cdot x \quad (2.4)$$

と表すことができる。

前提条件として与えたように、本システムでは、リーダの識別可能領域は 1 m^3 であり、 2.5 m/s の速度で搬送する高速なベルトコンベア上の物品識別を考える。このとき、通信は再送を含めて 400 ms 以内に完了しなければならない。

ここで、再送数 k は式 (2.3) における $P(n, r, \xi, x)$ に大きく影響するため、 k を増やすことが望ましい。しかるに、受け入れられる最大の通信時間 $\tau = 400 \text{ ms}$ を境界条件とすれば、 k が増加すると x を減少せざるをえない。これは P_t については P_r の劣化を引き起こす。 P_r と P_t を十分小さく保ったまま、少なくとも 4 回の送信試行が可能な TS-CDMA のパラメータは Table 2.1 にまとめられている。両端を除く二つのパラメータセットでは $l_i = 128$ 、 $l_c = 16$ 、 $\xi = r \cdot x = 1,024$ のとき 400 ms 以内に通信が完了する。通信時間と送信試行数のトレードオフを考慮にいと 16 bit の拡散符号長がここでも最適である。

データが失われる確率は、拡散符号長 $n = 16$ 、CDMA による平均多重数 $r = 4$ 、スロット数 $x = 256$ 、ならびに送信試行数 $k = 9$ のとき最小値を示し、およそ 2.53×10^{-9} となる。そのため、再送を 9 回とすると計 10 億個のトランスポンダに対して識別できないものは 1 個以下となり、実用上十分な性能である。

2.4 超多重 RFID の回路方式

2.4.1 トランスポンダの構成

Figure 2.8 はトランスポンダのデータ処理におけるフローチャートを表す。また、Figure 2.9 は設計したトランスポンダのブロック図を示しており、Analog Front-end (AFE) と Digital Back-end (DBE) から構成されている。AFE はアンテナに直接接続されており、受信した AC 電力を DC

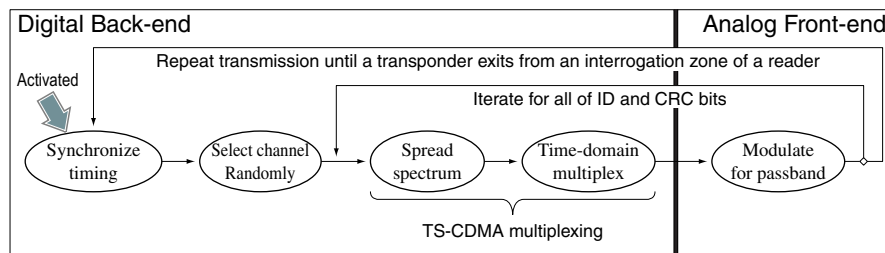


Figure 2.8: トランスポンダのデータフロー図

に整流してキャパシタにチャージする。また、電力供給波から同期信号を取り出すとともに送信信号を変調する。一方、DBEはFigure 2.8に示すように、TS-CDMA 多重信号とCRC 誤り検出符号を、内蔵のROMに格納されたID データから生成する。多重化されたビット列はAFEに渡され一次変調される。重要な構成要素について本節に記述する。Figure 2.9のトランスポンダAFE ならびにDBEの各要素について以下に記す。

2.4.1.1 トランスポンダの AFE

同期制御 提案する通信手法では、トランスポンダとリーダの間で同期を取ることは不可欠である。なぜならばトランスポンダから受信した拡散されたID データは、一定の時間内にリーダ内で生成された拡散符号と相関を取られなければならないからである。ここで、大きな演算資源を必要とするタイミング抽出や同期追跡機構を排除するため、リーダは電力供給波の位相を 180° シフトしたパルスを一周期だけ送出して通信開始を通知する手法を用いる。この手法によってトランスポンダとリーダ双方が同期した時間枠の中で動作することができる。

タイミング抽出回路はFigure 2.10(a)に示す通り、Set-Reset Flip-flop (SRFF) と Data Flip-flop (DFF) を使って実現することができる。回路の理想的な動作についてはFigure 2.10(b)に示されている。電力波が 180° シフトしたとき、SRFF の “set” 入力が続して二回立ち上がり、2周期の間SRFF の出力は high を保持する。DFF のクロック入力 SRFF の “set” に接続されているので DFF の状態は二回目の立ち上がりの時に high に遷移して一周期の間それが保持される。この単純な回路によって電力波の反転による同期タイミングを検出することが可能である。

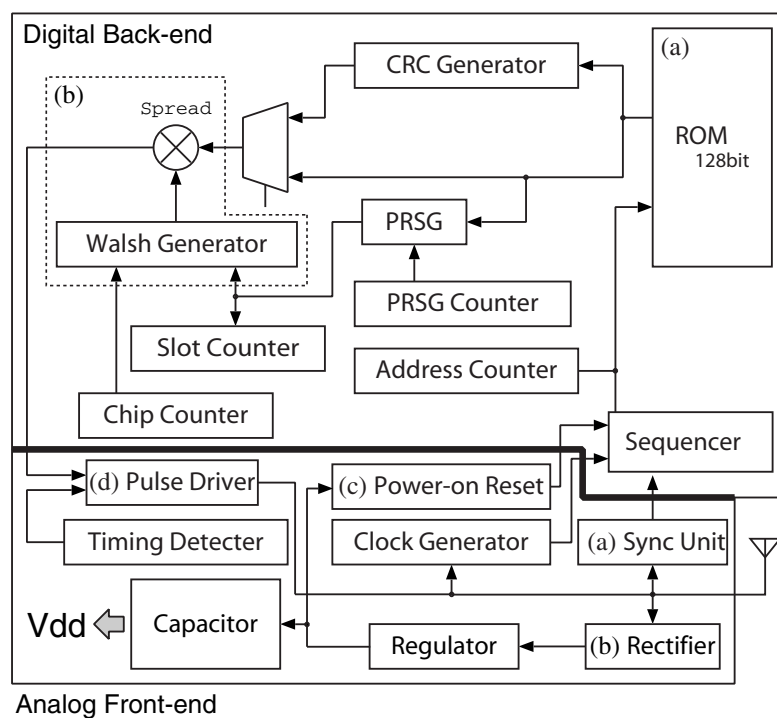


Figure 2.9: トランスポンダのブロック図

動作電力の確保 トランスポンダは電磁誘導則に基づいてリーダより 13.56 MHz の正弦波による電力供給を受ける。この電力波はリーダのアンテナから輻射されると磁界または電界の変化を引き起こし、この電磁界の変化がトランスポンダのアンテナに電流の変化を引き起こす。ここで、デジタル回路は DC 電圧で動作するので、トランスポンダは受信した AC 電圧を整流する必要がある。整流にはバイファイラ巻きのコイルを用いてセンタータップをグラウンドに落すダイオード全波整流器を用いた。整流された電力はトランスポンダが内蔵するキャパシタにチャージされて、デジタル回路の電源として使用される。

Power-on Reset トランスポンダの DBE は通信の制御を行うシーケンサを内蔵しているため、Power-on Reset (PoR) 回路が必要である。PoR としてシュミットトリガ・インバータを用いる。シュミットトリガの持つ、立ち上がりと立ち下がり異なる閾値電圧において出力遷移を伴うヒステリシス特性によって、外乱の干渉に対するロバスト性を高めることができる。トランスポンダはキャパシタにチャージされた電圧が「動作可能

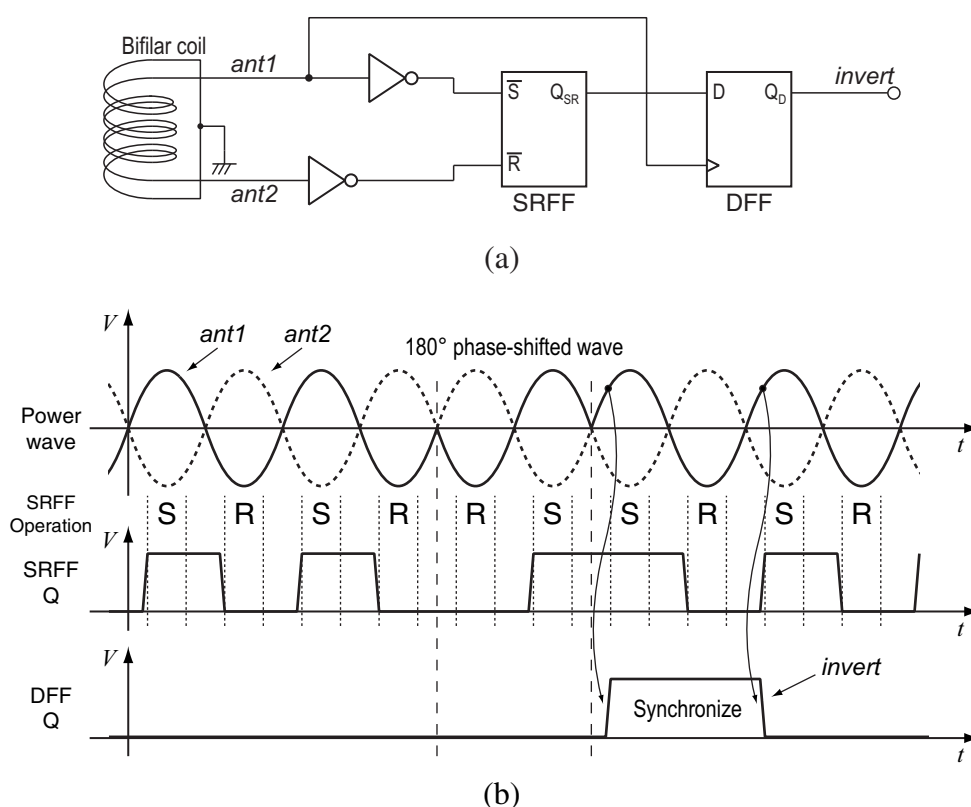


Figure 2.10: 位相シフトの抽出による同期制御の概要: (a) 回路図、(b) 動作フロー図

な」電圧に達すると直ちに動作を開始しなければならないが、いったん動作が開始されると電力供給の不安定性に影響されてはならない。電力波の予期しない歪みによって DBE がリセットされるのを避けるために、シュミットトリガ・インバータは立ち上がりの閾値をトランジスタ製造プロセスが規定する標準動作電圧、立ち下がり閾値を最悪動作電圧に設定される。Figure 2.11 の上半分にノイズなどの不安定要素によって歪んだ電力波を示す。一方、このときシュミットトリガ・インバータに期待される出力を下半分に示す。

電圧制限 RFID システムは電磁結合によりリーダーからトランスポンダへ電力を送る。DBE に供給される電力は電磁誘導されてトランスポンダのキャパシタにチャージされているものであるが、このとき LC 共振

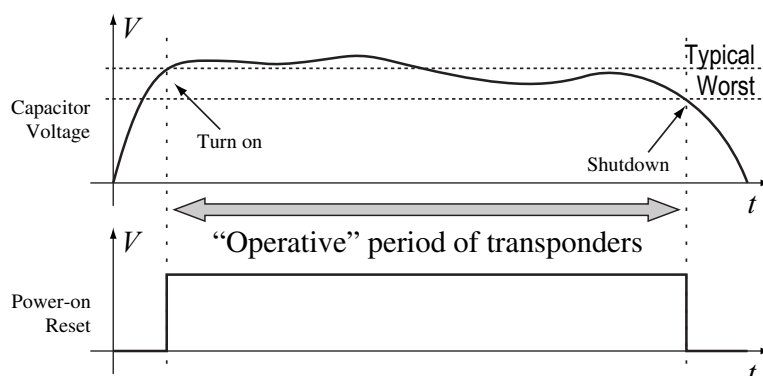


Figure 2.11: シュミットトリガによる PoR の動作模式図

することによって金属酸化膜半導体電解効果トランジスタ (Metal Oxide Semiconductor Field Effect Transistors; MOSFET) の絶対定格を超える電圧が印加される可能性がある。ダイオード・クランプが動作電圧を制限し、トランジスタの破壊を防ぐことで回路の信頼性を向上するために用いられる。クランプするダイオードの数はトランジスタの標準動作電圧によって変わる。たとえば、 $0.18\ \mu\text{m}$ の Complementary MOS (CMOS) テクノロジに回路実装した場合、ダイオードの数は3となる。クランプはその両端電圧が $1.8\ \text{V}$ を超過したときに有効になって、流れる電流量が急速に増加し、回路を保護する。

一次変調 一次変調器は Figure 2.12に示すように、二つの PNP バイポーラ接合トランジスタ (Bi-polar Junction Transistor; BJT) を用いる。BJT のコレクタはバイファイラコイルのそれぞれ両端に接続されていて、エミッタはともにトランスポンダの回路に電力供給するキャパシタに接続されている。これら BJT はベース電流によって電源からアンテナへ流れる電流の制御を行う。Figure 2.5に示すような正負両方のインパルスを生成するため、それぞれのアンテナ端に接続された二つの BJT は DBE からのベース電流によって排他的に on になり “0” および “1” の出力パターンに応じてパルス生成を行う。

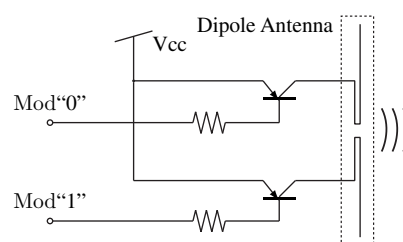


Figure 2.12: BJT によるトランスポンダの一次変調器

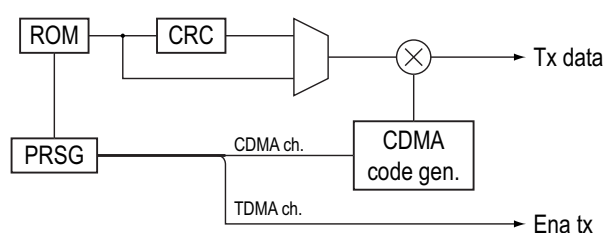


Figure 2.13: トランスポンダ側 DBE のブロック図

2.4.1.2 トランスポンダの DBE

トランスポンダの DBE 回路のブロック図を Figure 2.13 に示す。構成要素のそれぞれについて本節で説明する。

ID 格納メモリ RFID システムは「そこに何かがあるのか？」を各トランスポンダに一意に割り当てられた ID 番号を用いて識別するため、トランスポンダにおいては不揮発性のメモリが必要である。本方式においては、トランスポンダは同期タイミング以外の情報をリーダーから受け取らない。よって ID データの格納用メモリはマスク ROM により実装すると想定する。すなわち、トランスポンダの ID 番号は製造時にあらかじめ割り当てられチップに内蔵されとする。

TS-CDMA 多重化 各トランスポンダは Walsh 符号系列生成器と XOR ゲートを TS-CDMA 方式で変調するため、また PRSG をチャネルを選択するためそれぞれ内蔵する。通信チャネルは初期値として ID 番号を用いた PRSG で決定される。直交性のある拡散符号系列は割り当てられた符号番号をもとに Walsh 関数 [95] によって与えられて、XOR ゲートで ID

番号を拡散するため用いられる。拡散された ID データはクロックカウンタが割り当てられたスロット番号と一致するときに一次変調器に送られて送出される。

Walsh 符号系列は以下の Hadamard 行列から生成することができる。

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}, H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}$$

上記の生成規則に従って漸化的に生成した Hadamard 行列から、1 行または 1 列を取り出した数列が Walsh 符号系列である。Walsh 符号は自己相関が 0 となる直交符号である。そのため、拡散データの符号による相互干渉を低く抑える事ができる。

PRSG トランスポンダはチャネル番号の選択に 12 bit の PRSG を内蔵している。そのうち 8 bit がスロット番号を示し、残る 4 bit は拡散符号番号を示す。PRSG は M 系列の線形帰還シフトレジスタ (Linear Feedback Shift Register; LFSR) で実現することができる。LFSR のフィードバック・タップは系列のビット長が 12 bit のとき [6 8 11 12] である。PRSG は真性乱数ではないので、PRSG により生成される乱数系列は初期値によって決まる。チャネル衝突を削減するためには初期値の選択が重要である。RFID では全トランスポンダが重複しない値として ID 値を持っているので、これを初期値として用いることで解決される。

CRC エンコーダ 誤り訂正のため、トランスポンダは 16 bit の CRC 生成を要求される。CRC エンコーダも LFSR を用いて設計し、その系列長とフィードバック・タップは 16 および [5 12 16] である。ID ビット列を全て送信し終わったら CRC エンコーダが動作を開始する。エンコーダの出力は ID データ同様に TS-CDMA 方式によって多重化され送信される。CRC エンコーダをトランスポンダに内蔵する代わりに、あらかじめ ID に応じた CRC 符号を求めておき、製造時にマスク ROM に ID 番号とともに書き込んでおくこともできる。しかし、マスク ROM のメモリ空間が増えるためにシーケンサとカウンタによる回路面積や消費電力が増大するため、CRC 符号の場合はエンコーダを内蔵するほうが望ましい。

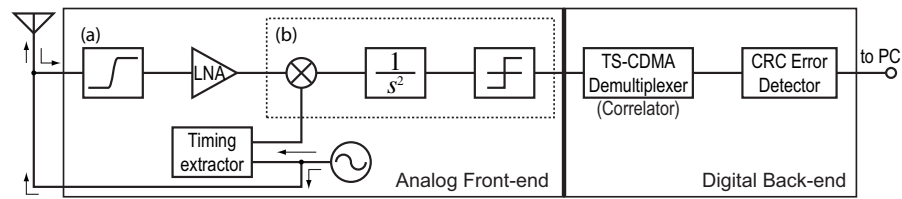


Figure 2.14: リーダのブロック図

2.4.2 リーダの構成

リーダの回路設計は Figure 2.14 に示すブロック図にまとめられている。電力供給のためにリーダはオシレータを内蔵しており、アンテナに直接接続されている。さらに、フィルタ、低ノイズ増幅器 (Low-noise Amplifier; LNA)、二重積分器、コンパレータと TS-CDMA の復調器を含む。受信信号から高域通過フィルタ (High-Pass Filter; HPF) を通し同じアンテナから送信される電力波成分を除去する。変調信号は LNA を通って増幅され、復調のため二重積分される。復調信号は単純にコンパレータを通すことでデジタルに変換される。送信された ID データは TS-CDMA 復調と CRC 誤り検出を含むデジタル信号処理によって復元される。最終的に誤りのない ID データだけがデータベースへと送られる。リーダの AFE における重要な構成要素として、Figure 2.14(a)–(b) に示される要素ならびに DBE について以下に説明する。

2.4.2.1 リーダの AFE

電力波除去用 HPF 一次復調の前にリーダは HPF を用いて電力波を除去する。なぜならば、リーダは電力供給に用いるアンテナを信号の受信にも用いるからである。トランスポンダの応答による周波数成分は、変調信号がインパルスであることから電力波よりずっと高い。そのため、HPF を通ることによって電力波だけが減衰される。

一次復調器 二重積分を用いたインパルス復調器を提案する。入力されたモノサイクルパルスは最初の積分によってガウスインパルスに変換され、二回目に三角波となる。二重積分によるチャネルノイズの干渉を削減するために、復調器では変調信号のみを抽出する必要がある。このた

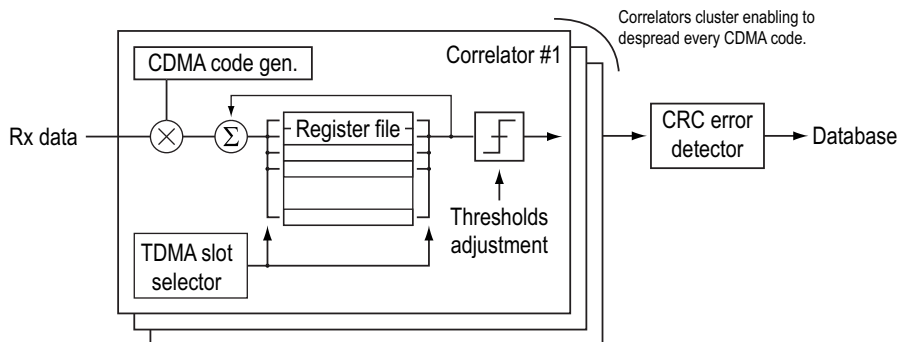


Figure 2.15: リーダに内蔵される相関器のブロック図

めにミキサを用いる。ミキサの LO¹¹ に抽出すべきタイミングにのみ立ち上がるデジタルパルスを入力することで、ミキサがスイッチのように働き変調された信号だけを通し、ノイズをブロックする。

2.4.2.2 リーダの DBE

リーダーの DBE のブロック図を Figure 2.15 に示す。本節では構成要素として TS-CDMA 向け符号相関器について説明する。

TS-CDMA 方式の相関器 回路には一次変調からのビット列が入力される。リーダーは拡散符号数と同じだけ、たとえば拡散符号が 16 種類あれば 16 個の相関器を内蔵する。それぞれの相関器は一意的な拡散符号を保持しており、その符号により拡散された受信信号に対して反応する。相関器は受信ビット列と拡散符号を積和演算することによって相関値を求める。このとき、TS-CDMA 方式では CDMA のチップそのものが TDMA により多重化されているので、ビットごとに演算結果をレジスタファイルへ FIFO¹² 方式で格納する。符号長だけ演算を繰り返したのちに、内蔵のコンパレータにより正／負の閾値とレジスタの演算結果を比較することで受信信号が “1” か “0” かを決定する。逆拡散されたデータはリーダーが内蔵する SRAM¹³ に格納され、CRC 符号によって誤り検出される。すなわち、逆拡散された ID データと CRC 符号から成るビット列に対して CRC

¹¹Local Oscillator

¹²First-In First-Out (先入れ先出し)

¹³Static Random Access Memory

演算を行い、結果がゼロとなることを確認する。誤りがなければデータベースへ送られる。

2.5 回路方式の設計検証

2.5.1 回路レベルシミュレーションによる検証

はじめに、SPICE 回路シミュレータを用いて一次変調による物理的な相互作用についてシミュレーションを実施した。Figure 2.16(a) に示すように回路を抽象モデル化し SPICE に記述を与えた。これによって取得した波形を (b) に示す。抽象化された回路モデルは変調用の PNP BJT がそれぞれのポールに接続されたダイポールアンテナの等価回路を含む。受信側と送信側のアンテナ間における結合係数を 0.01 とおく。BJT のベース端子は α および β とラベル付けられているが、それぞれが正と負のインパルス変調を行うため BJT を駆動する。Figure 2.16(b) は受信側のアンテナ端 γ で見られる受信信号を示す。変調信号はダイポール対ダイポール接続を通して受信側に送信されている。

一次復調を確かめるため、MATLAB 数値シミュレータを用いて環境ノイズのあるチャンネルにおけるデータ伝送のシミュレーションを行った。このとき、ダイポールアンテナの等価的なモデルを MATLAB に組み込む代わりに、Figure 2.16 で SPICE により与えられた受信信号を取り込み使用した。Figure 2.17(a) に、設計した MATLAB Simulink モデルを、また (b) に受信パスの様々な点におけるシミュレーション結果を示す。

この回路レベルモデル化は AFE の振る舞いを近似しており、以降の章で述べる高位モデル化において物理的な通信特性、たとえば信号レベルや信号対ノイズ比 (Signal-to-Noise Ratio; SNR) といった受信側から見積もることのできるパラメータの決定には欠かせない。

2.5.2 プロトタイプ実装

RFID システムの部分的なプロトタイプとしてトランスポンダ回路のテスト用集積回路 (Integrated Circuit; IC) チップを試作した。チップの回路方式は 2.4 節で説明したものに基づいている。この IC チップはトランスポンダの回路方式における基礎的な動作を検証することを意図して設計された。そのため、システム全体の機能性を実証することを意図して試作されたものではなく、PRSG や CRC エンコーダ、ID データ用 ROM など

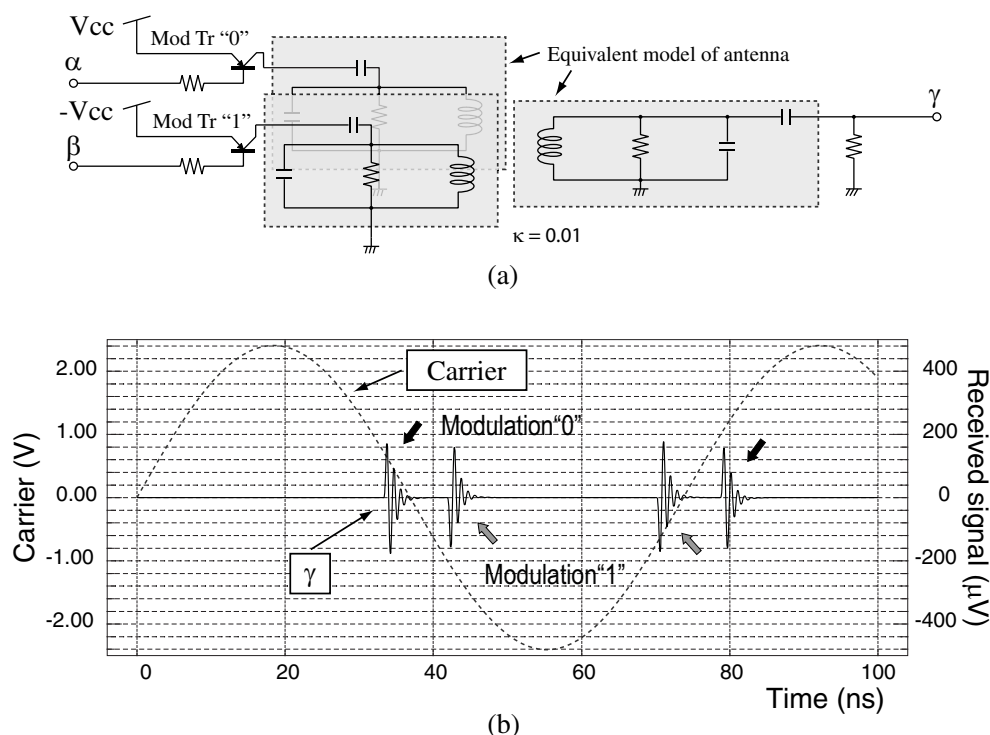


Figure 2.16: SPICE による回路記述: (a) SPICE 向け物理相互作用モデル、(b) 受信信号のシミュレーション結果

いくつかのモジュールは実装されていない。チップ写真を Figure 2.18に示す。実装面積は $800 \mu\text{m} \times 800 \mu\text{m}$ である。アナログとデジタル間での回路動作に伴う相互結合を排除するため、アナログ回路はデジタルから離れた場所に配置してあり、その間には合計で 100 pF のキャパシタセルが配置されている。

2.5.2.1 AFE

プロトタイプチップに搭載したトランスポンダの AFE を Figure 2.19に示す。2.4.1節に説明されている全ての構成要素は、バイファイラ巻きのアンテナである L_R と共振用のキャパシタ C_R から成る LC に直接接続されている。動作の詳細を以下に述べる。誘導結合によって供給された AC 電力を (1) に示される二つのダイオードで整流して DC にする。整流された DC 電力は (2) のキャパシタ C_P にチャージされる。この C_P は DBE の電力消費に対して十分な容量がある。(3) に示される三つの直列ダイオー

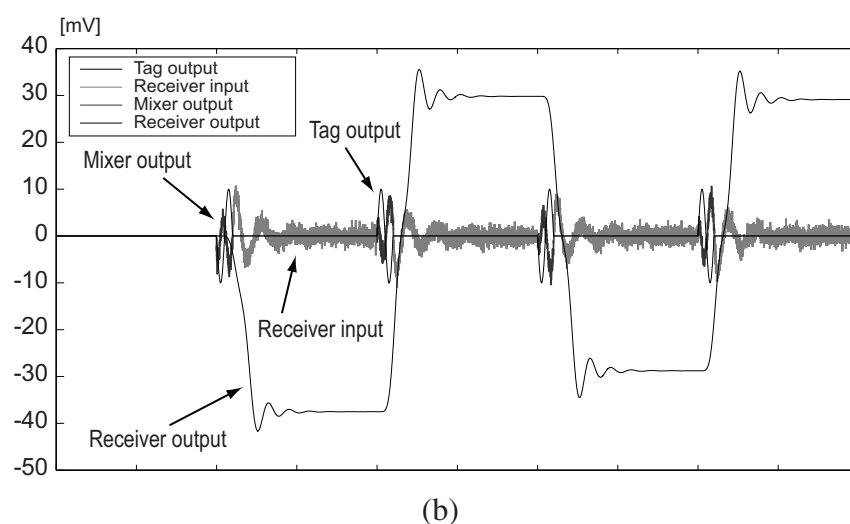
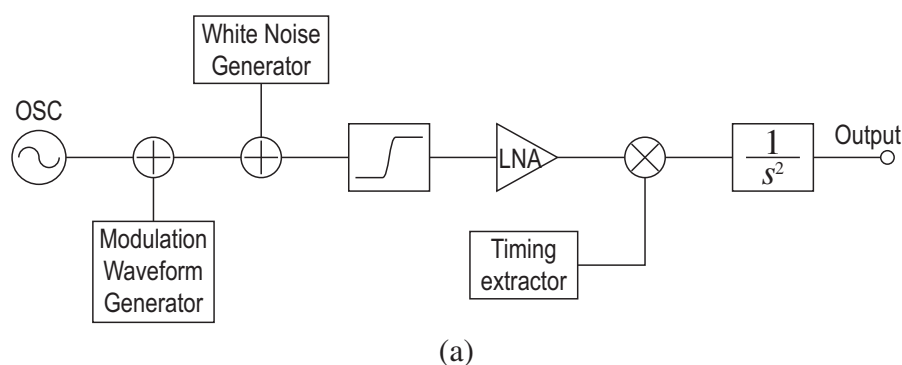


Figure 2.17: MATLAB による回路レベル記述: (a) リーダの等価モデル、(b) シミュレーション波形

ドは DBE の電源電圧を 1.8 V にクランプする。PoR 回路としては (4) に示されるようにヒステリシスなシュミットトリガ・インバータが実装されている。また、リーダーからの電力波によってロジック回路をリセットするタイミング信号を生成する。同期タイミングの抽出には (5) の SRF 与 DFF による同期コントローラが設計されている。

2.5.2.2 DBE

DBE には Walsh 生成器、スペクトル拡散器、シーケンサとカウンタが実装されている。2.4.1.2 節で説明されている構成要素の中では、TS-CDMA 多重化のみがチップに含まれている。PRSG や ID ROM を含まないため、

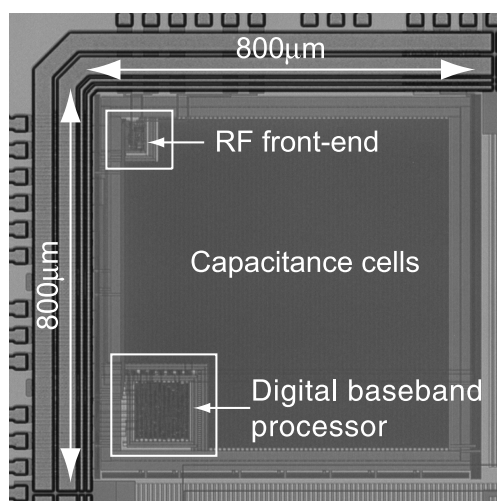


Figure 2.18: テスト用トランスポンダのチップ写真

ID 番号や拡散符号番号、スロット番号を外部測定器によって生成する必要がある。この DBE は $0.18\ \mu\text{m}$ CMOS プロセスの標準セルライブラリを用いて 123 セルに論理合成され、自動配置配線ツールによってレイアウトされた。

2.5.3 実験による基礎検証

Figure 2.19 に示されるトランスポンダの設計結果によってレイアウトからネットリストを抽出し、HSPICE ならびに Nanosim を用いて回路をシミュレーションを実施した。シミュレーション波形を Figure 2.20 に示す。この波形は同期タイミングの前後だけ抜粋されたものである。波形 A、B、C、D はそれぞれ Figure 2.19 において対応するラベルの付加された点で観測されたものである。波形 A と B はバイファイラ巻きアンテナの直後で受信された電力波である。波形間の位相はちょうど 180° シフトしている。2 段目の波形は変調タイミングを示す。これは電力波がゼロと交差する近傍において high に遷移する波形であり、これに基づいて BJT がインパルス変調を実現する。3 段目は抽出された同期タイミングであり、4 段目はキャパシタ電圧である。AC の電力波から $1.8\ \text{V}$ の DC 電圧が整流により得られていることが示されている。

続いて、試作したチップを用いてプロトタイプシステムを作成し実測評価した。Figure 2.21 に実測環境を、Figure 2.22 に結果を示す。システ

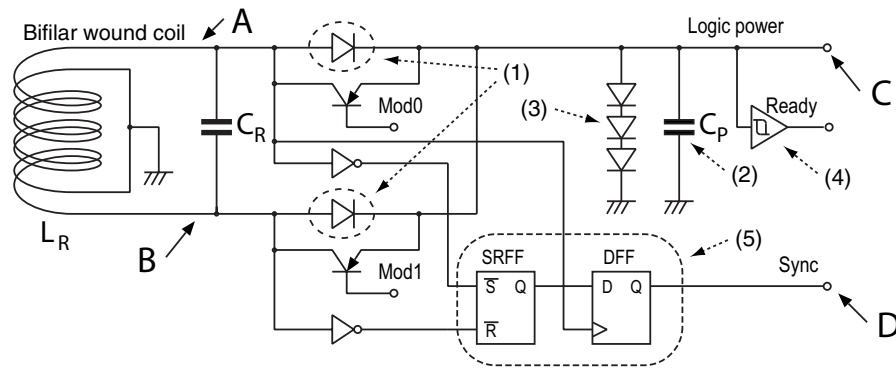


Figure 2.19: トランスポンダの RF 回路図: (1) 整流器, (2) キャパシタ, (3) 電圧クランプ, (4) PoR, (5) タイミング抽出

ムの動作を明らかにするため、ここではオシロスコープによる取得波形を二つ示す。Figure 2.22(a) は DBE の出力を示しており、Figure 2.22(b) は AFE の出力を示している。

Figure 2.22(a) の下部に示される同期パルスが high になった直後、上部の TS-CDMA 多重回路の出力パルスは
 “0011001100110011–1100110011001100” と読むことができる。ここで、外部から与えられた Walsh 拡散符号は “0011001100110011” であったため、このパルス列は “01” が拡散されたものであることを意味している。

波形 (b) は同じ拡散符号を与えたときのインパルス変調を示している。上部の波形は拡散符号であり、下部は変調器から出力されアンテナ輻射される変調信号である。矢印であらわされるインパルスが変調信号である。取得された波形は、アンテナから輻射される際にダイポールのスルーレートによって変換され、Figure 2.5に示される波形となる。2.5.1節で説明したシミュレーション結果から明らかなように、この受信インパルスはリーダ回路によって復調することができる。

したがって、回路レベルにおける等価モデルのシミュレーション結果ならびにプロトタイプの実測結果から提案した回路方式の有効性が示された。

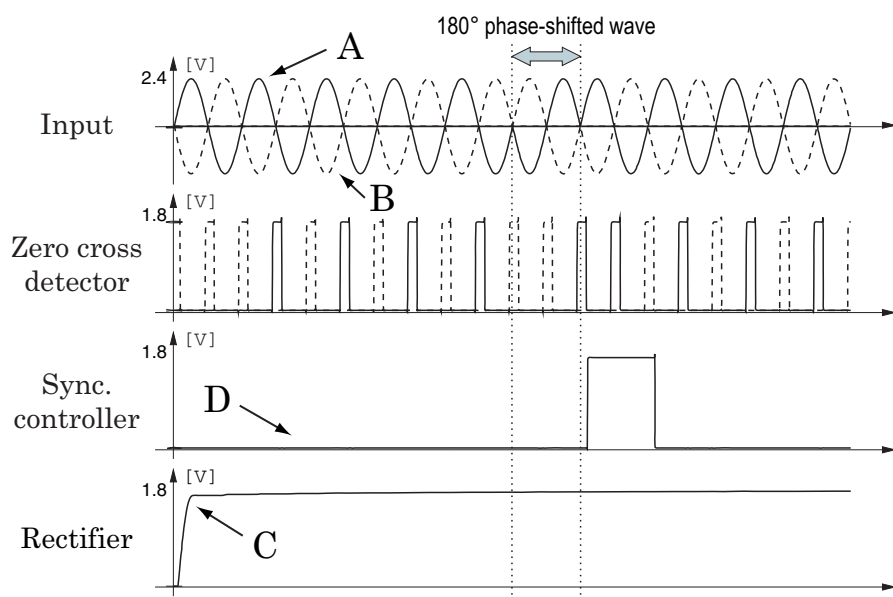


Figure 2.20: トランスポンダ側 AFE のシミュレーション波形

2.6 結言

本章では、物品の識別を高速に行うことを意図する衝突防止アルゴリズムを考案した。このアルゴリズムはTS-CDMA多重化、CRC符号による誤り検出、再送による誤り回復から構成される。提案アルゴリズムは確率的手法に属しており、トランスポンダがPRSGを内蔵することによって、チャンネル割り当てをランダムプロセスに基づいて自発的に行うことによって、決定的手法で必要となるトランスポンダへの指令を排除することに成功した。この衝突防止アルゴリズムはランダムプロセスに基づくため、衝突確率を完全にゼロにすることはできないが、数理的な分析を与え通信パラメータを導出した結果、理論的な誤り率は 2.52×10^{-9} と十分に低いことを実証した。また、衝突防止アルゴリズムに基づく通信方式とそれを実現するための回路方式を導出した。回路方式の検討にあたっては全体像を定めてから詳細を詰めていくトップダウン・アプローチを用いた。このため、高機能性と簡素な回路方式を保ったままシステム全体の設計が可能であった。PNP BJTを用いたインパルス変調も、このアプローチによって導出した。一方、設計に際してはボトムアップ・アプローチよりも広い視野における考察を行った。具体的には、回路レベル

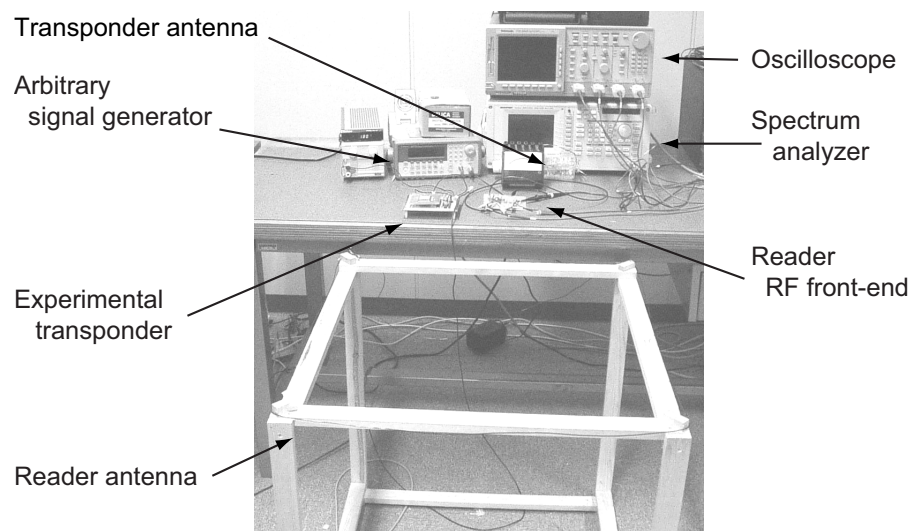
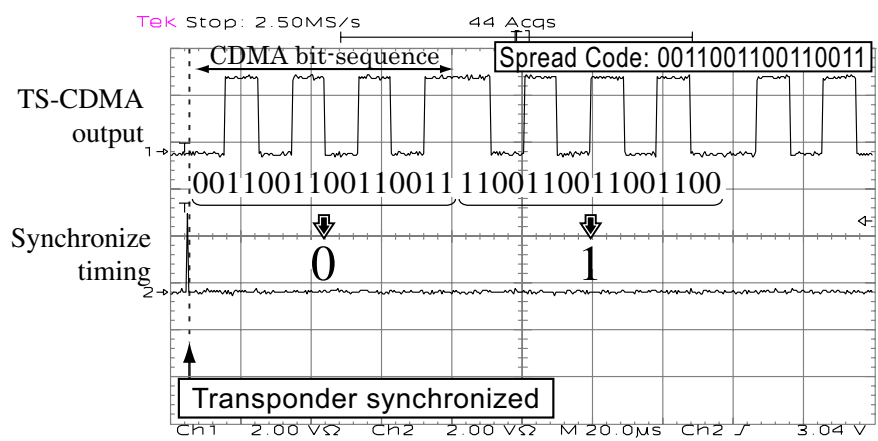
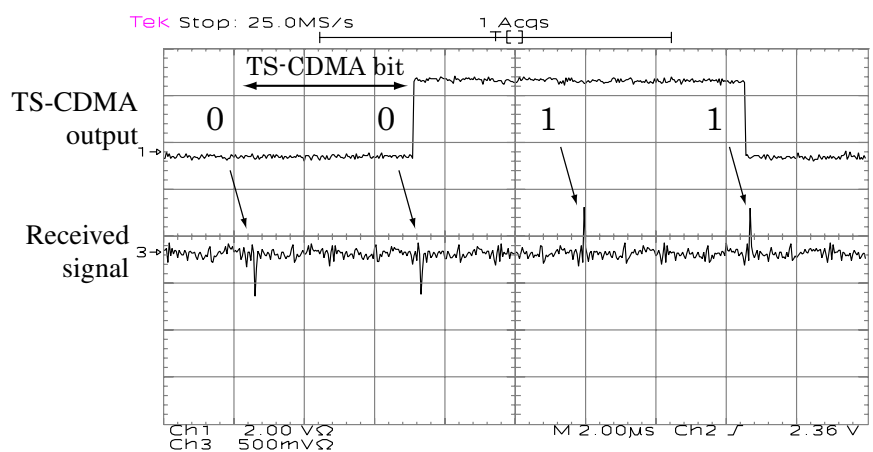


Figure 2.21: 実験環境の写真

シミュレーションにより等価モデルを使って設計検証を行い、設計の妥当性を示した。また、試作チップにより設計回路の動作を確認した。以上に基づき、RFIDシステムの設計において高位モデル化手法の有効性が証明された。



(a)



(b)

Figure 2.22: トランスポンダとリーダ間の通信の実測結果 (a) DBE の出力、(b) AFE の出力

第3章

高位モデル化によるバックエンド設計手法の提案

3.1 緒言

前章では、超多重応答により認識効率を大幅に改善することができる通信手法について新たに提案を行った。その議論の中で、数理的な解析に基づき認識効率や誤り率の基礎的評価を得ることはできたものの、現実システムへの実装を考えるとさらに多くの評価項目の分析が必要である。数理モデルは理想的な状況に基づいて立式するため、現実に応じた状況に対して数理モデルによるアプローチは不適切である。実際の状況に応じた評価を行うためには実験システムを構築することが最も望ましいものの、超多重システムは単一のリーダに1,000を超えるトランスポンダが応答して成り立つため、その試作コストは他の衝突防止RFID¹と比べて非常に大きい。したがって、システム設計の早期段階で実験的に試作することもまた適切ではない。このため、擬似的な実験システムのシミュレーションまたはエミュレーションによる高位モデル化を行うことで現実的な状況に照らしたシステムの分析や評価が可能であると考えた。特に多重通信はデジタル処理を行うバックエンド回路によって実現されるため、その設計方針はシステムの性能に大きく関わる重要な要素である。すなわち、超多重RFID向け通信方式をそのデジタル信号処理において現実に応じた性能評価を行うためにバックエンドの高位モデル評価系を構築し、最適な多重通信パラメータを求める必要がある。

本章では高位モデル化に基づくシステムパラメータの最適化と、超多重通信におけるロバスト性の評価を通してバックエンドの設計手法を確立することを目的とする。この高位モデルとは、実際にハードウェアならびにICチップの設計において考慮する必要のあるシリコン物性あるいは具体的な回路方式を含まない、抽象度の高いシステムレベルにおける

¹Radio Frequency Identification

通信モデルのことを意味する。これは、本章における設計手法が実際にハードウェアがどのように実装されるか、トランスポンダがどのような回路方式で集積されるか、あるいはトランスポンダとリーダーの間の結合は電波伝搬かそれとも電磁結合か、どのようにトランスポンダはリーダーにID情報を伝送するのかといった具体的な議論に踏み込むことなく、多重通信性能を左右する衝突防止アルゴリズムの評価を通してバックエンド設計の導出を可能とすることを示している。したがって、本手法は抽象度の高い上位層（システムのアプローチ設計）から具体性の高い下位層（デジタル回路設計）に向けて抽象度を下げながら本章の目的であるバックエンド設計を行うトップダウン・アプローチである。

はじめに、ハードウェア・エミュレータによる多重通信の基礎的な評価系を提案する。次に、提案する評価系を用いて多重RFIDの通信におけるロバスト性の評価を行う。さらに、ソフトウェア・シミュレータによるロバスト性の評価系を提案し、最後に提案する評価系を用いて1,000を超える多重通信のロバスト性に関する評価を行うとともにデジタル多重処理におけるロバスト性を考慮した最適パラメータを導出する。

3.2 ハードウェア・エミュレータによるビヘイビアモデル

3.2.1 ノイズによる応答信号の減衰

Figure 3.1は、(a) ノイズのない理想的なチャネルでの通信、ならびに(b) ノイズのある実際のチャネルでの通信における波形の比較を図示したものである。図が示すように、通信の品質を下げる主な要因は四つ存在する。

第1はチャネルノイズによる電力供給波の振幅変動である。第2はこの振幅変動によって電力供給波のゼロ交差タイミングに生じる揺らぎである。これはトランスポンダの変調タイミングの揺らぎを引き起こす。第3としては第1に示した電力波の振幅変動と同様、トランスポンダの応答における信号振幅の変動であり、チャネルノイズに起因する。これは、応答信号の強度が受け取った電力波から整流されトランスポンダ内に蓄えられたチャージ量に依存するからである。これらの3つの要因は主に通信チャネルにおける白色ノイズに起因する。そのため、白色ノイズは実際の環境における通信品質を評価する際に特に考慮する必要がある。第4

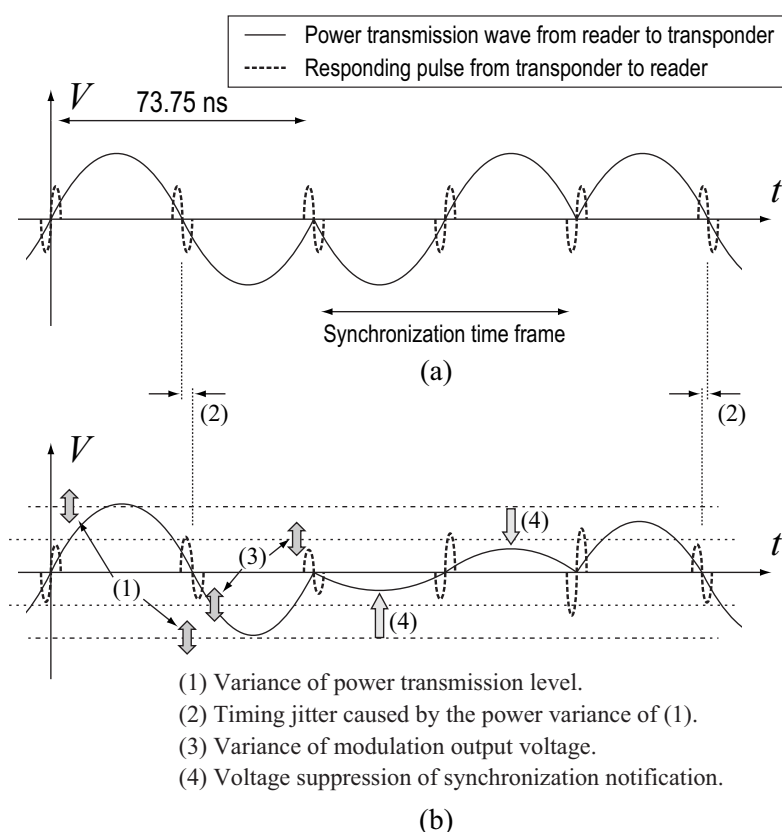


Figure 3.1: チャンネルノイズの有無による波形劣化: (a) ノイズのない理想的なチャンネルでの通信、(b) ノイズのある現実的なチャンネルでの通信

の要因として、同期タイミングにおける振幅の低下が電力波の輻射電波とその反射波の衝突によって引き起こされる。これは通信を不確かにさせる。しかしながら、電力波の反射は波形生成回路とアンテナの間におけるインピーダンス整合によって最小化することが可能である。

以上より通信品質を下げる一番の要因は白色ノイズである。しかし、チャンネル内を多重化されて送られるトランスポンダからの応答は1,000を超えるため、多重通信に関するパラメータをシミュレーションすることは困難である。このような多重通信のためのシミュレーションを行うためには非常に多大な演算資源と時間が必要である。そこでエミュレータを用いてこの問題を解決した。エミュレータによる専用の高速計算でノイズのある通信チャンネルを想定したときのRFIDシステムのパラメータを評価することができ、実際の環境における最適なパラメータセットを

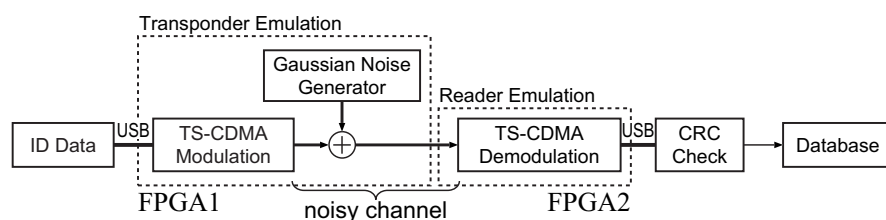


Figure 3.2: エミュレータのブロック図

導出することが可能である。本節では、提案した RFID の多重通信をデジタルレベルでビヘイビアモデル化して構築した通信チャネル評価用のエミュレータについて説明する。

3.2.2 アーキテクチャ

本節では、これまでに行った理論的な分析を確かめるとともに、通信チャネルに環境ノイズを含んでいる実際のシステム性能を評価するため、Field-Programmable Gate Array (FPGA) を用いて構築した超多重 RFID 向け通信手法のエミュレータの開発手法について説明する。

Figure 3.2に構築したエミュレータのブロック図を示す。Figure 3.3に例示するように、各々USB²ポートを備えた二枚のFPGAボードから成る。このとき、一方のボードが1,000個のトランスポンダを模擬し、もう一方が受信側の逆拡散を模擬する。これら二枚のボードはデジタルで直結されているため、環境ノイズのある疑似通信チャネルはデジタル表現によりモデル化される。送信側のFPGAボードはUSBポートを経由してPCから全トランスポンダのIDビット列を与えられる。一方、受信側はUSBを通してPC³に相関結果すなわち逆拡散したデータを転送する。また、トランスポンダ群を模擬するFPGAの出力ポートはリーダの相関器群を模擬するFPGAの入力ポートと接続されている。

3.2.3 リーダ・ユニットの構成

Figure 3.4はエミュレータに実装されたリーダ回路のブロック図を表す。提案した通信方式では、Table 2.1に示すように最適な拡散符号数を

²Universal Serial Bus

³Personal Computer

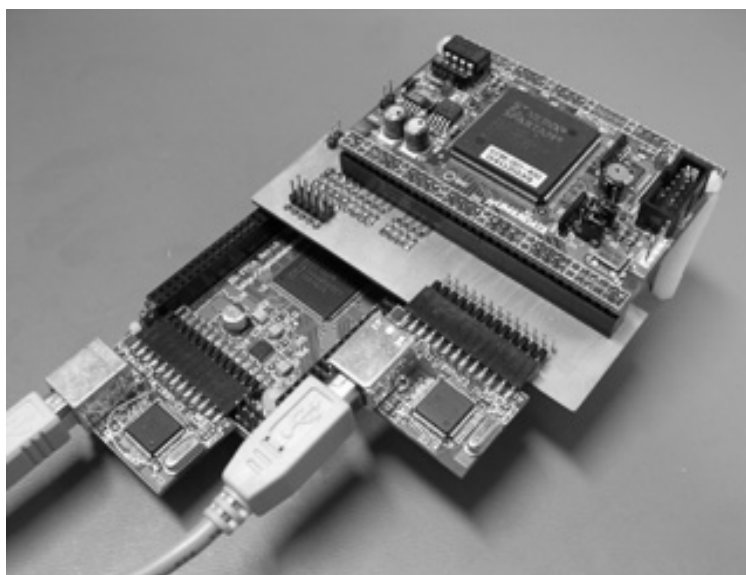


Figure 3.3: エミュレータの写真

16 と求めた。そのため、その 16 種類ある拡散符号それぞれに対応する 16 個の相関器が内蔵されている。相関器は受信した信号と拡散符号を掛け合わせることで符号相関値を導出し、これを 512 個から成る 10 bit の TDMA⁴チャンネル値レジスタに先入れ先出し (First-in-first-out; FIFO) 方式にて記録する。拡散符号長は 16 bit なので 512 スロットのそれぞれに対する相関値は 16 回求められ、レジスタの値に累算される。レジスタから出力される 10 bit の値は受信したビット情報の各拡散符号に対する尤度を表す。10 bit の分解能を持つ内蔵コンパレータは、この尤度に対して正／負の閾値を用いて受信したビットが “1” であるか、また “0” であるかを決定する。その閾値はチャンネルの状態に応じて適切に調整される。逆拡散後のデータはリーダ側エミュレータ・ボードに内蔵されている RAM⁵にいったん記録され、再送が行われている間にコンピュータに転送される。CRC⁶符号による誤り検出は作業用に大量のメモリ領域が必要となるため、CRC 誤り検出機能はエミュレータ・ボードから切り離し、コンピュータ上に実装した。つまり、逆拡散された ID はコンピュータに転送された後に正当性が確認されることになる。また、リーダ側エミュレータは拡

⁴Time Division Multiple Access

⁵Random Access Memory

⁶Cyclic Redundancy Check (巡回冗長検査)

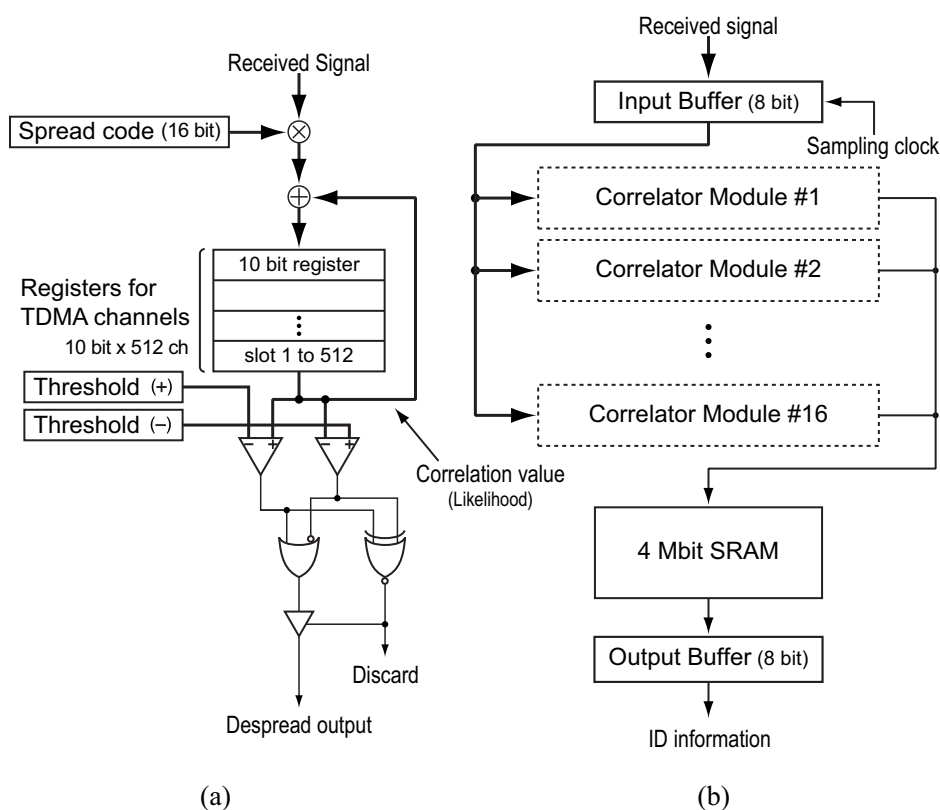


Figure 3.4: リーダの逆拡散プロセスのブロック図: (a) 相関器、(b) 逆拡散モジュール

散符号と相関を取って 1 bit でも閾値を超えない ID を破棄する。

3.2.4 トランスポンダ・ユニットの構成

Figure 3.5は、トランスポンダ群エミュレータに内蔵されるトランスポンダ・ユニットのブロック図を示しており、128 bit の ID データをランダムに選んだスロットと拡散符号によってデジタル的に変調する。また、その ID は 16 bit 単位に分割され乱数の初期値として PRSG に与えられる。1,000 個のトランスポンダからの応答をエミュレートするために、それぞれのユニットからの変調出力は仮想的に合成され、擬似的な通信チャンネルを通してリーダ側エミュレータに与えられる。このエミュレータは仮想的に 1,000 個のユニットを内蔵しており、それぞれのユニットが持つ ID は PC に構築されたデータベースにて設定され、USB 経由で与えられる。結果

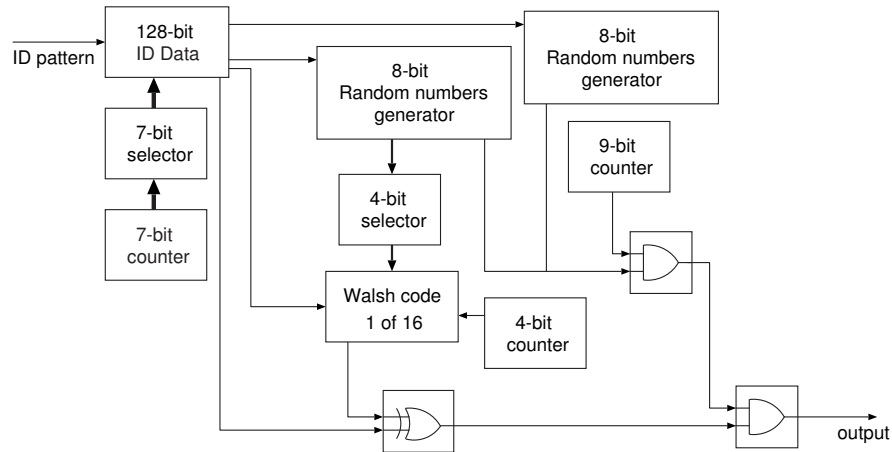


Figure 3.5: トランスポンダの拡散プロセスのブロック図

として、エミュレータの出力はTS-CDMA⁷変調を実施した後のトランスポンダによる応答をデジタル化し、時間軸上で足し合わせたものを示す。

3.2.5 疑似チャネルの実現

電磁伝搬を考慮すると、通信方式を評価しRF⁸回路を設計するにあたってチャンネルノイズの影響を調査する必要がある。このような状況で最も影響する要因が白色ノイズであるとの想定に基づき、Figure 3.6に図示する疑似ガウスノイズ生成器をエミュレータに実装した。

LFSR⁹の出力する乱数は一様に分布するので、これは白色ノイズ生成器と見なすことができる。複数のLFSRによる出力を加え合わせることで、その確率密度は正規分布に近くなる。これは中心極限定理[96]に基づいている。

以上より、八つのLFSRによる出力を加算することで疑似ガウスノイズ生成器を設計した。また、それぞれのLFSRにおける相互相関が発生しないように、各LFSRのフィードバック・タップや初期値は乱数系列ごとに異なるよう設定した。LFSRの長さは8であり、これはトランスポンダが出力するビット長に等しくなるように定められている。生成された疑似ノイズはトランスポンダの送信信号にデジタル的に加算されて受

⁷Time Slotting-Code Division Multiple Access

⁸Radio Frequency

⁹Linear Feedback Shift Register (線形帰還シフトレジスタ)

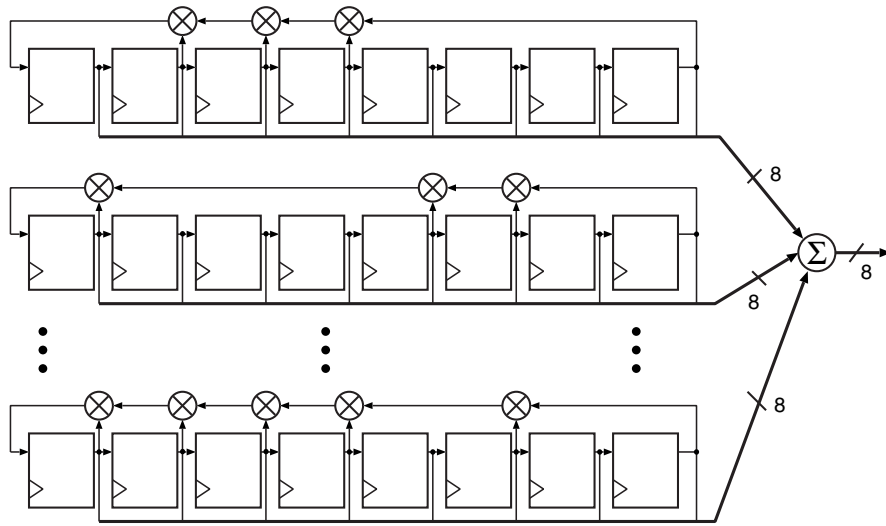


Figure 3.6: 疑似ガウスノイズ生成器のブロック図

信側に送られる。

3.2.6 TDMA チャンネルと再送数の関係

2.3.6節に記述した通信時間の制約を満たしつつ、最も適切な多重通信パラメータを導出するために、ノイズのないチャンネルを通るときの送受信をエミュレートすることで、ID 誤り率 (ID Error Rate; IDER) を導出した。チャンネルの割り当てをランダムに行うために PRSG¹⁰として 16 bit の LFSR を用いて、その乱数系列の初期値を毎回の送信試行のたびにトランスポンダ ID の異なるビット位置から抽出して用いることとした。Figure 3.7は通信時間と IDER の間の関係を示している。ここで、TDMA スロット数として 512 と 256 の場合を求めた。

Table 2.1に示す通り、提案パラメータを用いて式 (2.3) から理論的に求められた誤り率はおおよそ 10^{-9} である。しかし、エミュレーション結果によると、512 スロットの場合 400 ms の通信時間での誤り率は 10^{-2} より大きくなると求められた。これは、LFSR に基づく PRSG によるチャンネル割り当てが真性乱数によって行われていないことによる。このような疑似乱数の性質は、IC¹¹上にトランスポンダを実装するにあたってデジタ

¹⁰Pseudo Random Sequence Generator (疑似乱数生成器)

¹¹Integrated Circuit (集積回路)

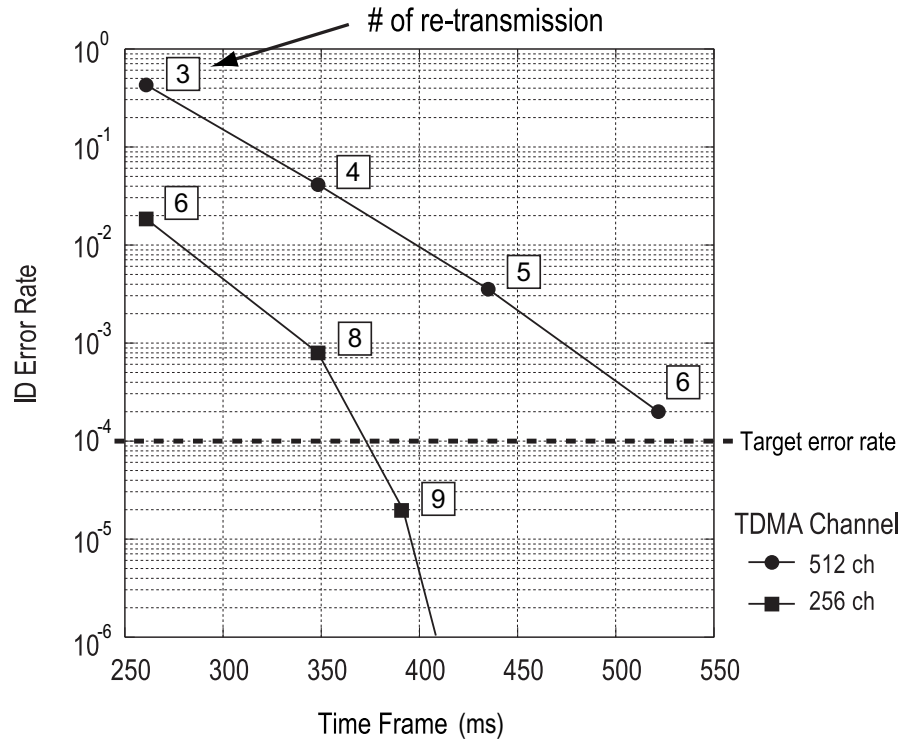


Figure 3.7: TDMA チャンネルによる IDER への影響

ルの乱数生成を行う限り、避けることができない重要な要因である。目標とする誤り率を $IDER < 10^{-4}$ 、すなわち 10,000 個のトランスポンダを認識する際に誤って伝送される ID 数を 1 未満と設定するならば、512 スロットの場合で 6 回の再送が必要であることが図に示されている。しかるに、この 6 回の再送を行うと通信時間が 400 ms より大きくなるため高速識別には適切でない。一方、スロット数を 256 とおくと $IDER < 10^{-4}$ を満たす再送数で誤り率は大きく削減することができる。これらの観測結果は 2.3.6 節において行った理論的な予測と一致している。エミュレーションから導出されたシステムパラメータを Table 3.1 にまとめる。これは Table 2.1 と対応する。

結論として、多重アクセス環境におけるチャネルノイズのエミュレーションはシステムの通信性能を評価し、通信時間と誤り率の制約をともに満たすことのできる最適なシステムパラメータを導出するにあたって効果的なアプローチであることを示した。

Table 3.1: エミュレーションによるシステムパラメータの性能諸表

	Emulated	
n :# of Spread code	16	16
r :# of CDMA ch.	2	4
x :# of TDMA ch.	512	256
t_{TX} :Time frame [ms]	348.1	391.5
k :# of re-transmission	4	9
P_c :IDER	4.1×10^{-2}	1.9×10^{-5}
$(P'_c$:IDER – Ideal)	3.7×10^{-7}	2.5×10^{-9}

3.2.7 閾値によるノイズへのロバスト性

相関値が閾値を超えるかどうかによってビット値が決定されるため、相関演算においては正および負の閾値は非常に重要な役割を果たしている。それゆえ、正 (+) および負 (-) の閾値は受信信号の変動により影響されないように適切に調整される必要がある。

相関器の閾値を 1.00 から 0.50 までパラメータとして取ったときの IDER と SNR¹² の間の関係を Figure 3.8 に示す。エミュレータにおいてはノイズをデジタル的に加えるため、SNR は

$$\text{SNR} = 20 \log \left(\frac{\sum_{k=0}^{10} 2^k i_k}{2^s \cdot \sum_{j=0}^8 2^j e_j} \right)$$

と与えられる。ここで、トランスポンダ側エミュレータの出力を

$$i_{10}i_9 \dots i_0 (i_k \in \{0, 1\})$$

また、ノイズ生成器の出力を

$$e_8e_7 \dots e_0 (e_j \in \{0, 1\})$$

とおく。また、ノイズ生成における論理的なシフト調整を s とする。閾値はノイズを考慮せず完全に相関が取れたとするときの相関値、すなわち正の閾値が 16 で負の閾値が -16 をそれぞれ 1.00、 -1.00 として正規化した値とする。実際のシステムにおいては通信チャネルのノイズレベルをあらかじめ求めておくことはできない（ただし推測はできる）ので、こ

¹²Signal-to-Noise Ratio (信号対ノイズ比)

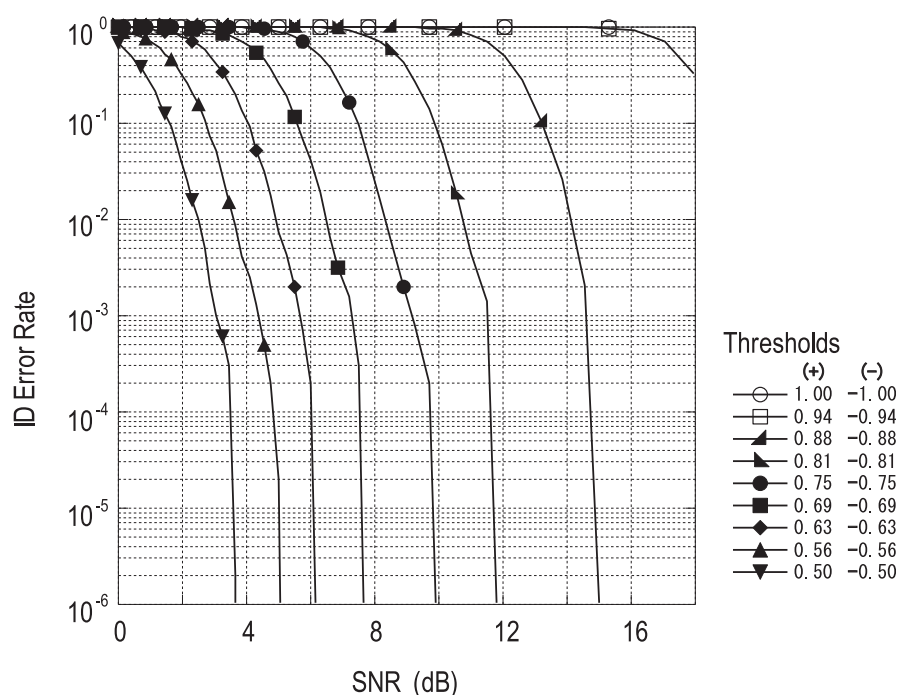


Figure 3.8: 閾値を変化させたときの IDER と SNR の関係

の場合の閾値は通信チャネルの SNR を推測して適宜に調整されなければならない。たとえば、チャネルの SNR がおよそ 5 dB であると仮定すると、適切な相関器の正規化した閾値は 0.56 と -0.56 である。Walsh 符号は直交性を持ち自己相関がないため、ノイズのないチャネルでは閾値を 1.00 ならびに -1.00 と設定すればよい。

Figure 3.8の結果から、閾値が下がるほど IDER が減少しているという事実が明らかである。CRC による誤り検出数、すなわち不正確に伝送された ID の数をそれぞれの閾値において求め、結果を Figure 3.9にまとめた。正しくない ID の数はおよそ 800 前後で最大を示す傾向がある。この数にはトランスポンダとリーダ間の通信において誤って伝送された ID のみならず、相関器において誤って逆拡散された ID も含まれており、リーダから PC へ送信される ID 総数はトランスポンダ数の合計である 1,024 をはるかに超える。閾値が 0.63 より大きい場合、SNR の劣化に伴って誤った ID 数も減少する。この理由は、ノイズの存在するチャネルにおいて受信信号の変動が大きくなったとき相関結果はちょうど閾値前後でばらつき、よって CRC の誤り検出に到達する前に破棄されるからである。

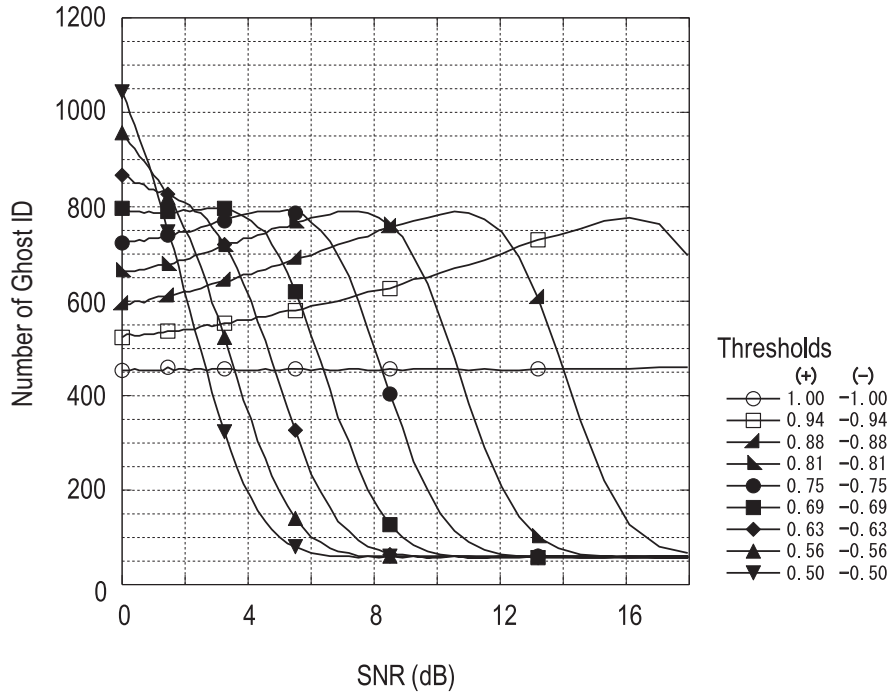


Figure 3.9: 閾値を変化させたときの SNR と誤って伝送された ID 数の関係

Figure 3.9は同時に、誤って伝送された ID のためにリーダにおいて作業用メモリに少なくとも 800×144 bit の容量が余分に必要となることを示している。それゆえ、通信チャネルの SNR が 5 dB より大きいノイズを考慮すると、通信における信頼性は 300 kbit のメモリを実装することで実現可能であることが結論づけられた。

3.3 ソフトウェア・シミュレータによる高位モデル

3.3.1 シミュレータの概要

前節で説明したエミュレータにより多重通信の性能とガウス性の白色ノイズに対するロバスト性の評価が可能となった。しかしながら、通信チャネルにおけるノイズは白色性のものだけでなく、インパルス性のものや他の通信機器による電波障害など様々な性質のものを考慮する必要がある。そこで、エミュレータに加え様々な外乱に対する多重通信シス

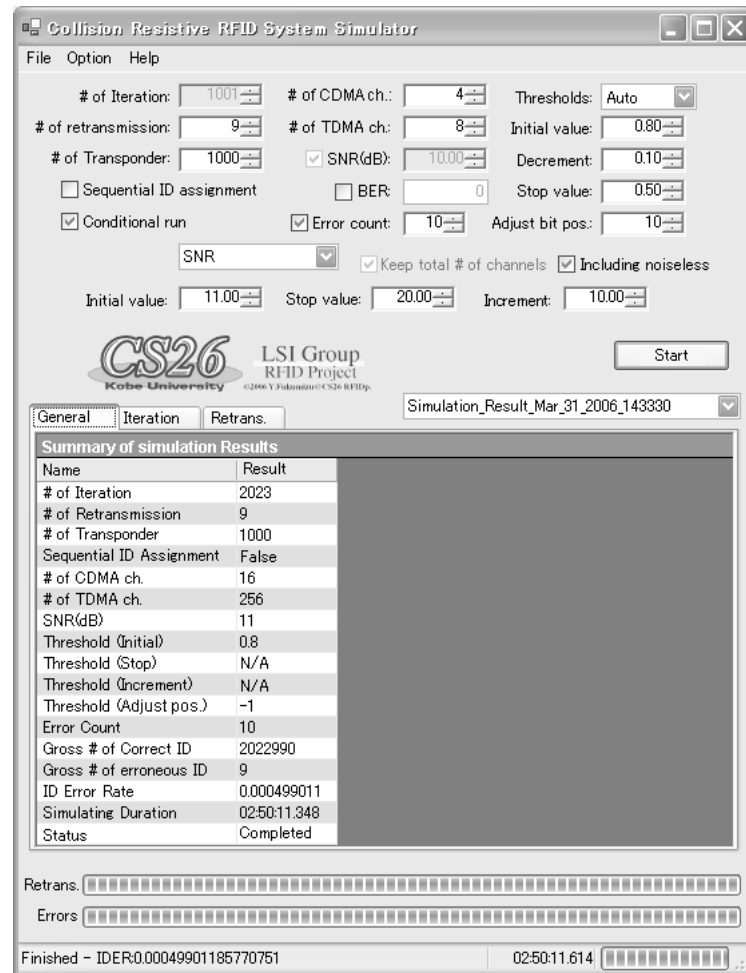


Figure 3.10: シミュレーションシステムのスクリーンショット

テムのロバスト性をより詳しく分析・評価するため、ソフトウェアによるシミュレーションシステムを構築した。このシミュレータは複数のトランスポンダと単一のリーダーで仮想的に通信を行わせることにより、衝突確率および誤り発生率をモンテカルロ法に基づく確率値として導き出す。

このシミュレーションシステムは Microsoft Windows の .NET Framework 1.1 上で実装した。スクリーンショットを Figure 3.10 に示す。シミュレーションパラメータは Graphical User-Interface (GUI) を通じて柔軟に設定することができるので、システムの幅広い動作状況に応じた誤り発生率を導き出すことができる。

構成する仮想的な RFID システムの動作を可能な限り現実のシステム

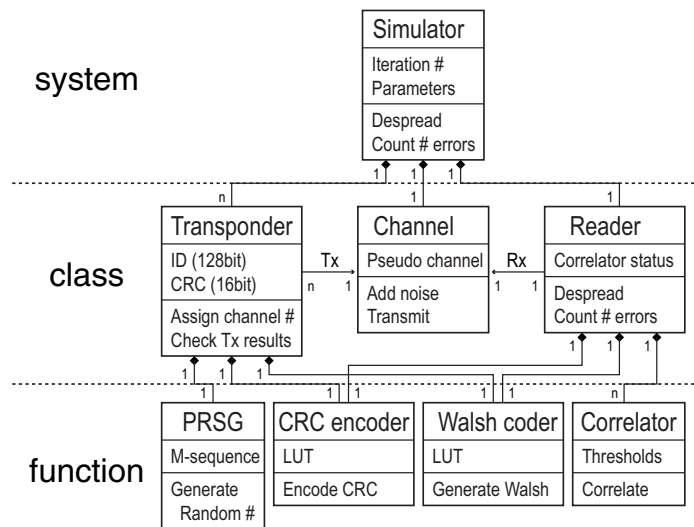


Figure 3.11: シミュレーションシステムの構成図

に近づけるため、シミュレータは C# 言語を用いてオブジェクト指向プログラミング (Object-Oriented Programming; OOP) により実装されている。シミュレーションシステムは Figure 3.11 に示される通り、主に3つのクラス、すなわちトランスポンダクラス、チャネルクラス、リーダクラスから構成される。各クラスはそれぞれ実際のモジュールと同等の機能性を提供する。これによって、理想的な状態だけでなく現実に即した環境におけるシステム動作を模擬することが可能となっている。

3.3.1.1 トランスポンダクラス

トランスポンダクラスはランダムに割り当てられた ID を含むオブジェクトである。このクラスにおいては内蔵メカニズムによって TS-CDMA チャネルを割り当てて、チャネルクラスに CDMA で変調された信号を出力する。ここで、“TS-CDMA チャネル” とは TDMA による時分割スロットと CDMA による拡散符号を組み合わせた多重チャネルを意味する。シミュレータは同時通信数と同じだけのトランスポンダクラスをメモリ上に確保し、個別に ID 送出を行わせる。なお、このシミュレータは最大で 65,536 個のトランスポンダを模擬することが可能である。各トランスポンダは CRC エンコーダ、PRSG、Walsh 符号 (拡散符号) 生成器を内蔵するべきであるがこれらの基本機能は占有メモリ量を削減するためにす

すべてのトランスポンダクラスで共通のものを使用する。また、適宜テーブルルックアップを適用することでシミュレーション速度を高速化する。

3.3.1.2 チャネルクラス

多重化通信チャネルのシミュレーションを行うために、チャネルクラスが定義されている。このクラスは各トランスポンダクラスから出力信号値を受け取って疑似チャネルを模擬的に伝搬させ、リーダに受け渡す。チャネルクラスはすべてのトランスポンダによる通信を TS-CDMA 方式にしたがって多重化して単一の配列に格納し、通信環境の白色ノイズを加える。得られた多重通信値はリーダクラスに引き渡される。このクラスの実装を修正することによって、実際の物理的性質に即した様々なシミュレーションを柔軟に実施することが可能となる。たとえば、各々のトランスポンダに重み係数を導入することによって、リーダ応答範囲内を移動しているトランスポンダのリーダアンテナとの距離に応じて起こる信号劣化を模擬することができる。

チャネルクラスは、ソフトウェアの柔軟性によりノイズ成分として様々な性質のものを伝送信号に注入することが可能であるが、本節では簡単のため白色ノイズのみに限定して以下の分析を行う。また、このとき各トランスポンダとリーダアンテナとの距離はすべて等しいと想定した分析結果を示す。これは非常に理想的な状態であって現実的ではない。それでもなお、最適な設計パラメータを調査することは可能であり、これによって高位モデル化手法の有効性を示す。なお、構成したシミュレータにおいては個々のトランスポンダに個別の重み係数を割り当てることで信号強度の分散を模擬することも可能である。

3.3.1.3 リーダクラス

リーダクラスはチャネルクラスから受けとった多重信号値を復調してから相関関数を用いて TS-CDMA 方式により逆拡散し、誤り検出する。可能性のあるすべてのチャネルを逆拡散する必要があるため、リーダクラス内に割り当てられる相関器クラスの数を実行する多重通信における CDMA チャネル数に等しく、各相関器には逆拡散過程に必要な個別の Walsh 符号が割り当てられている。リーダクラスがチャネルクラスよりデータを受け取ると、それをすべての相関器クラスに分配する。相関器は受信データと Walsh 符号の積和をとって TDMA チャネル別に用意された配列に FIFO 方式で記録することでその相関値を導出する。言い換

えれば、個々の TDMA チャンネルに対応する FIFO バッファが相関器に確保されている。そして、それぞれの TDMA チャンネルごとの相関値がバッファメモリに蓄積される。Walsh 符号列との積和を取り終えると、相関器は閾値判定によって ID ビットを決定する。リーダクラスは、この逆拡散結果を CRC 誤り検出関数に基づいて誤り検出する。最終的にトランスポンダから受信した ID はデータベースと照合して実際に送出された ID と等しいことを確認する。一方、正しく逆拡散できて CRC による誤り検出も通過したにも関わらず、データベース内にあるいずれの ID とも一致しない場合がある。これは、いわゆるゴースト ID の存在を確認するためである。これらは TS-CDMA による多重通信において TDMA/CDMA チャンネルが衝突することによって起こるものであり、トランスポンダがランダムでチャンネルを選択する限り、確率的に発生する誤りである。当然ながらゴースト ID は誤った ID とみなされる。

3.3.2 シミュレーションシステムの動作フロー

Figure 3.12(a) はシミュレータを構成するそれぞれのクラスが行う通信動作を示している。Figure 3.12(b) はシミュレーション実行中に表示される通信状況ウィンドウのスクリーンショットである。このウィンドウは通信中の全トランスポンダ ID の通信状況をリアルタイムに表示する。ここに表示される受信状況は3種類あり、(1) 正常に受信できた ID、(2) 受信機の相関器で逆拡散できなかった ID、(3) CRC により誤りが検出された ID を表す。これらの誤りに関するデータとゴースト ID の数はシミュレーションが完了した後に計数され、誤り発生率が求められる。

この通信状況ウィンドウを観測することで各トランスポンダの通信状況が明らかとなり、直感的にパラメータの調整を行うことができる。たとえば Figure 3.12(b) に示したスクリーンショットでは、およそ 80% のトランスポンダが正しく通信できており、18% が相関器で積和演算を行った結果、閾値誤りを起こしている。また、残り 2% は CRC によって通信誤りが検出されたことを示している。

3.3.3 1,000 を超える RFID 多重通信の解析と設計

本節では、シミュレーションによる様々な解析を通して 1,000 を超える多重 RFID 向け通信システムの最適な設計パラメータセットを抽出する方法を示す。

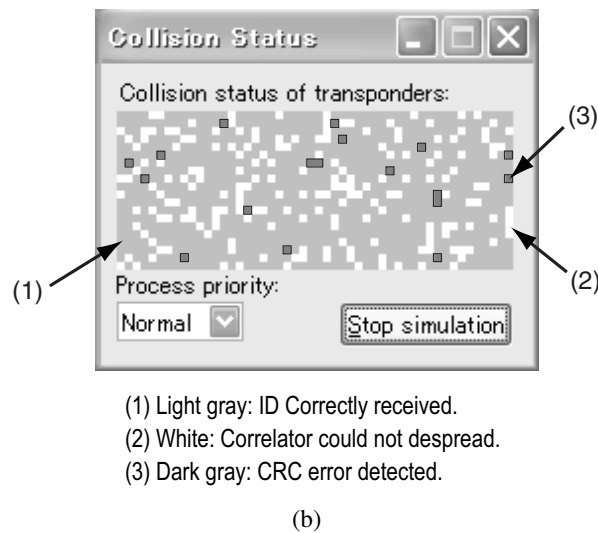
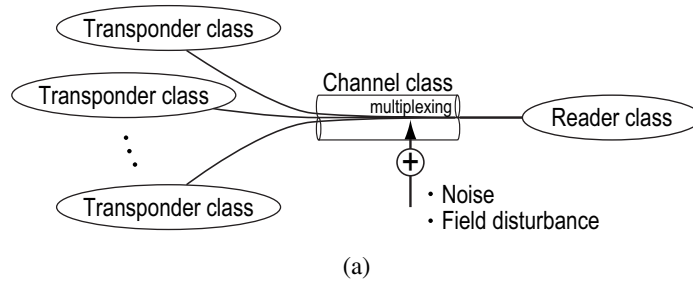


Figure 3.12: 多重通信シミュレーションの概要: (a) シミュレータの動作フロー図、(b) 通信状況ウィンドウのスクリーンショット

TS-CDMA による同時通信数は最大で $N = s \cdot c$ と定義される。ただし、TDMA スロット数は s 、CDMA 符号数は c であらわされる。 s あるいは c を増加することにより、TDMA/CDMA チャンネルを通じて同時送信可能なトランスポンダ数も同様に増加する。チャンネル衝突による通信誤りを削減するために、各トランスポンダは ID の送信が完了すると再送が始まる前に内蔵の PRSG によりチャンネル番号を再び割り当て直す。ここで再送数を x と定義すると、それぞれの ID の全ビットを送出するのにかかる時間 T_t は次のように与えられる。

$$T_t = T \cdot (l_{ID} + l_{CRC}) \cdot s \cdot c \cdot x$$

ただし、ID 長を l_{ID} 、CRC 長を l_{CRC} 、1 bit あたりの送出時間を T とする。チャンネル数が増加することによって、同時に識別できるトランスポ

ンダ数を増やすことができるものの、一連の通信にかかる時間 T_t はアプリケーションの運用上の制約に依存して一定であるため、チャンネル数と再送数の間にはシステム性能を左右する重要なトレードオフが存在する。

本節では基準として2種類の誤り量を定義する。すなわち IDER とゴースト ID 数 (Number of Ghost IDs; NGID) である。IDER は x 回の再送を行った後、すなわち T_t の通信時間の中で識別に失敗したトランスポンダの存在確率をあらわし、NGID は 3.3.1.3 節で定義したところのゴースト ID の再送数 x に対する比率である。これは衝突に伴って起きる潜在的な誤り発生率をあらわしている。

3.3.4 RFID 通信における外乱の影響

3.3.4.1 ノイズのある環境でのチャンネル衝突

通信時間 T_t が 400 ms 以下であり CDMA 符合数 c が 16 であるパラメータセットにおいて、TDMA スロット数 s が 512 の場合と 256 の場合の異なる 2 種類を想定し、環境ノイズつまり外乱の IDER に対する影響と再送数の関係を調査した。このとき再送は s が 512 のとき 4 回、256 のとき 9 回まで行うことができる。このときの環境ノイズとして SNR で 5、10、15 および 20 dB を注入する場合と、それに加えて環境ノイズを注入しない状況を想定した。結果を Figure 3.13 に示す。

Figure 3.13 から IDER が少なくなるにつれてチャンネルノイズによる影響が増大することがわかる。例えば、 T_t が 400 ms の近傍では、ノイズのない環境と SNR が 5 dB の環境では IDER が 10 倍近い差を示している。この図よりノイズレベルがどうあれ、再送数を増加することで IDER を軽減することができることが明らかになった。特に、誤り発生率の改善効果は TDMA スロット数 s を半減して、再送数 x を倍増した後者のパラメータセットのほうが高い。この誤り発生率の改善によってノイズによる影響を減らすことができる。

3.3.4.2 チャンネル容量

チャンネル衝突に対するロバスト性を評価するため、SNR で 20 dB のノイズのある通信チャンネルを想定し、トランスポンダ数を通信方式の想定する同時識別数である 1,000 から、その倍の 2,000 まで増やしつつシステムのシミュレーションを行って IDER を求めた。このとき、通信チャンネル数 $s \times c$ を 4,096、8,192、16,384、32,768 とした。前提条件として T_t

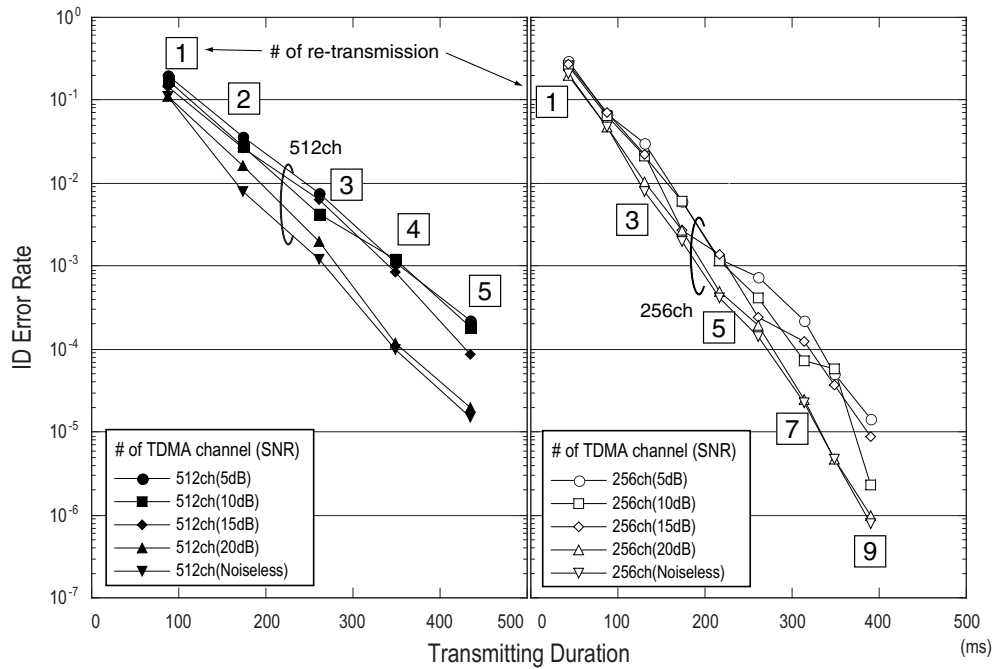


Figure 3.13: ノイズ環境下における IDER と TDMA チャンネル数の関係

を 400 ms と設定したので、再送数 x はそれぞれ 9 回、4 回、2 回、1 回と与えられる。Figure 3.14 に結果を示す。これによると、同時に通信するトランスポンダ数が多くなったとしても、チャンネル数を増加するよりも再送数を増加するほうがよい結果を示している。一方、再送を増やしてチャンネル数を減らすとトランスポンダの衝突確率そのものは高くなる。誤り率の劣化は、Figure 3.14 では曲線の傾きによって与えられ、チャンネル数が少ないとトランスポンダ数の増加に伴って急激に IDER の劣化が起こる。ここで、チャンネル数が 4,096、再送数が 9 回、トランスポンダ数が 2,000 個のとき IDER は 1.83×10^{-4} を示し、これはトランスポンダ数が 1,000 個のときに較べて約 100 倍の劣化が起きている。すなわち 2,000 個の同時識別につき 0.366 個の誤りであり、これはチャンネル数を 8,192、再送数を 4 回としたときの 1,000 個の同時識別の値とほぼ変わらない。よって、トランスポンダ数がシステムの想定するチャンネル容量を超過する場合においても、再送数を増やすことで IDER を改善できることが明らかになった。

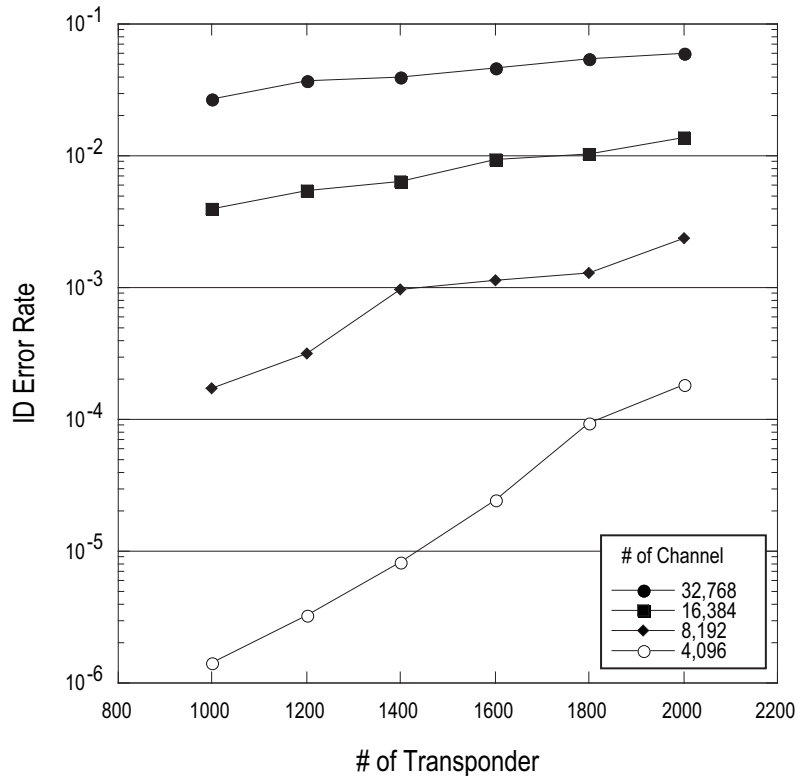


Figure 3.14: チャンネル容量と IDER の関係

3.3.4.3 TDMA/CDMA チャンネル分配

通信チャンネル数はTDMA スロット数 s と CDMA 符号数 c の積で与えられるが、これは送受信時間 T_t と再送数 x により制限されている。TDMA および CDMA チャンネル数の最適な配分を導き出すために、400 ms の通信時間において 9 回の再送を可能とするとの条件設定のもと、システムシミュレーションを実施した。システムのチャンネル総数は 4,096 である。 s/c の比率による IDER ならびに NGID の影響を導き出すため、この比率を変化させてシミュレーションを行った。結果を Figure 3.15 に示す。このときのノイズレベルは SNR で 10 dB と仮定した。

c が増加すると IDER は減少し、全チャンネルを CDMA に配分したとき最小値を示す。一方で、興味深いことに NGID は分配率に大きく影響されないことがわかる。よって CDMA 符号数を増やすことで IDER を削減することができるが、これは同時にリーダーの設計を困難にするとともに、

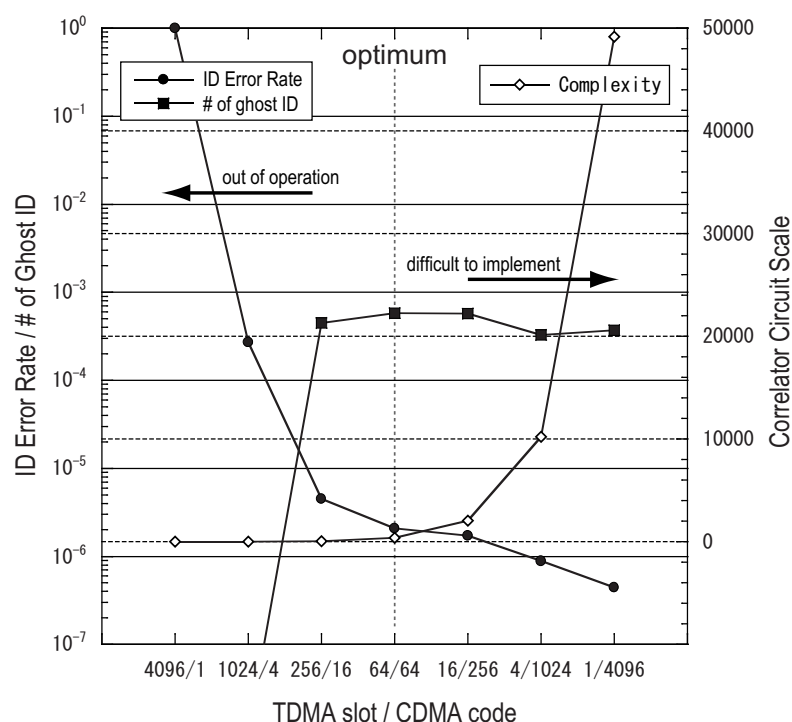


Figure 3.15: チャンネルの分配率による IDER/NGID への影響

トランスポンダの動作を不安定にすることになる。すなわち、リーダにおいて可能性のあるすべての CDMA 符号を並列して逆拡散しなければならないため、リーダに内蔵される符号相関器の総数は符号数に伴って指数関数的に増大する。もちろん、リーダの回路規模も同様に増大する。一方、トランスポンダは TDMA スロットを待つことによる間欠的な動作によって、外部にある電源からキャパシタへの非接触給電を確実にしているため、TDMA チャンネル数を減らすとトランスポンダの電力確保が問題となる。したがって、CDMA チャンネル数は誤り発生率の低減に寄与するが、これらの考察に基づいて制限される。以上の議論より $c = 64$ かつ $s = 64$ の場合がもっとも最適な分配であると考えられる。

Table 3.2: シミュレーションにより抽出された最適パラメータ

	Simulated
r :# of CDMA ch.	64
x :# of TDMA ch.	64
t_{TX} :Time duration [ms]	391.5
k :# of re-transmission	9
P_e : ID Error Rate (IDER)	2.09×10^{-6}
N_e : # of Ghost IDs (NGID)	5.79×10^{-4}

3.3.5 ロバストなRFID通信向けバックエンドの設計

AFE¹³の設計については2.4節において既に議論したので、本節では最適化されたDBE¹⁴処理を内蔵するトランスポンダの設計例について議論する。

外乱に対して十分なロバスト性のもと1,000を超える多重RFID通信を可能とする最適システムパラメータセットは前節の議論より導出することができた。まとめると再送数はチャネル数よりも誤り発生率の削減に大きく関与するとともに、環境ノイズが増加した場合やチャネル容量に対してトランスポンダ数が超過した場合のロバスト性の改善にも寄与する。Table 3.2に最適化したパラメータをまとめる。

本節で提案した設計手法を用いて求めたバックエンド設計と、その過程において最適化したシステムパラメータの実装性を確認するために、トランスポンダのバックエンドを0.35 μm CMOS¹⁵プロセスにて実装した。Figure 3.16に設計したチップ写真を、Table 3.3に設計データを示す。本チップはDBE回路を試験的に実装することが主目的であるが、それに加えてAFEで必要とするダイオードやBJTなどアナログ素子のTest Element Group (TEG)を兼ねているため内部パッドに接続された各アナログ素子とAFEもチップに実装されている。また、本チップのDBEは内部信号をモニタするために外部とデジタル入出力を行う。DBEが外部端子との間で安定した信号の授受を行うために、チップにはIOバッファおよびDBEと独立してIOバッファに電力を供給するための電源端子ならびにリングが実装されている。DBEの実装面積はIDデータを記憶する

¹³Analog Front-end

¹⁴Digital Back-end

¹⁵Complementary MOS

Table 3.3: トランスポンダチップの DBE の設計諸元

	Layout
Process	0.35 μm CMOS@3.3 V
# of transistor	10,558
Circuit scale	115,800 μm^2

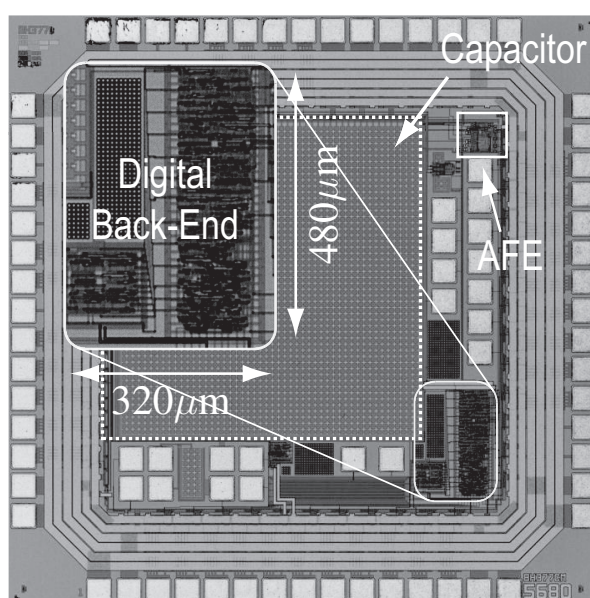


Figure 3.16: トランスポンダ DBE の設計チップ

ために実装したシフトレジスタを除外すると、およそ $240 \mu\text{m} \times 480 \mu\text{m}$ と十分に小さい。そのため、動作電力をチャージするための電源用キャパシタの実装を考慮したとしても、トランスポンダの回路面積を十分小さく抑えることが可能である。本チップにおいては実装面積の余剰分を全てキャパシタに割り当てたため、合計で 890 pF のキャパシタンスを実装することができた。DBE における消費電力は 128 bit のシフトレジスタを含めて 1 mW 以下に抑えられている。シフトレジスタがデジタル回路の実装面積において約 50% を占めることを考慮すると、DBE の消費電力は $500 \mu\text{W}$ を下回っており、これは、従来研究と比較しても多重 RFID のトランスポンダとして十分低電力である [51]。

1,000 を超える RFID 通信向けのバックエンド設計においては、3.3.4 節

で述べたような種々の外乱に対するロバスト性を確保するために多くのシステムパラメータを考慮する必要があるものの、これらのパラメータは本節で議論した高位モデル化手法を用いることで多角的に評価を行うことができ、その結果に基づいてトランスポンダのバックエンド設計を最適化することができる。また、本手法を用いたトランスポンダのバックエンド回路においても、トランジスタ数は十分低く抑えることが可能であり、本手法の有効性を実証した。

3.4 結言

本章では、バックエンド設計の側面から通信方式を評価しバックエンドに反映するための設計手法として2種類の高位モデルを導入した。2章で行った多重通信の評価は理論分析に基づくものであり、現実に応じた評価結果と乖離する。そこで、信号伝搬の劣化による性能への波及を調査するための環境として高位モデルを位置づけた。その1はハードウェア・エミュレータである。これは、通信方式を離散時間のデジタル表現でモデル化しFPGAに実装したもので、ノイズのある通信チャネルにおける現実に応じた性能指標を得ることができる。ノイズのあるチャネルにおいても再送の効果が実験的に確かめられ、そのときエミュレーションによって得られたIDERは 1.9×10^{-5} であった。エミュレーション結果からは相関器において閾値を調整することがノイズの存在するトランスポンダとリーダ間の通信において極めて重要な意味を持つことが示された。

その2はカスタムソフトウェアによるシミュレータである。ソフトウェアの柔軟性によって、複数のトランスポンダがあるRFIDにおいて、より多くの外乱要因に対するロバスト性の評価が可能となった。外乱による影響を考慮したときも、再送を行うことによって誤り率や通信チャネルの容量超過に効果的であることが確かめられた。チャネル配分の分析を通して、拡散符号数はノイズへのロバスト性に大きく影響する一方、NGIDはTDMAスロット数とCDMA符号数の比に影響しないことを見いだした。シミュレーション結果から最適なパラメータセットを抽出して、トランスポンダのバックエンド設計に適用した。その結果、回路規模を維持したまま、より適切な多重パラメータが実現できることを示した。これらの分析は、1,000チャネルのRFID設計において高位モデル化手法が効果的であることを証明した。

第4章

統合シミュレーション環境によるアナデジ混載チップの設計手法の提案

4.1 緒言

前章までの議論によって、超多重 RFID¹のための通信手法とそのバックエンドの設計手法が確立された。一方で、RFID システムは無線伝送を用いて実現されるため、変復調や電磁伝搬といったアナログ領域において信号処理に付随する通信劣化の要因や影響を詳細に分析する必要がある。しかるに、3章で提案した高位モデル化手法はエミュレータ、シミュレータいずれにおいてもデジタル領域の分析技術であり、外乱などの通信劣化をデジタル表現でモデル化する必要があった。ハードウェア・エミュレータはFPGA²を用いて実現されるため、アナログ処理は全く含むことができず、実装可能なハードウェア規模にも制約があった。また、ソフトウェア・シミュレータについてはアナログ処理についても動作レベルで抽象化することで多少は含ませることが可能であったものの、ハードウェア設計と対応づけられていないために、設計結果の検証手段として利用することができなかった。本章ではアナログ／ミックスドシグナル・シミュレーションモデルとカスタムソフトウェアによる高位モデルを結合することによって、アナデジ混載のハードウェア設計を統合することを目的とする。それにより超多重 RFID の外乱成分に対する現実に即したシステム性能の評価が可能である。はじめに3章で提案したシミュレータによる高位モデルを発展させた統合マルチレベルシミュレーション環境を提案する。次に、この統合シミュレーション環境の特徴を明らかにするため3章で提案した高位モデルとの比較を行う。さらに、この統合環

¹Radio Frequency Identification

²Field Programmable Gate Array

境により2章で提案した超多重RFID向け通信方式をシステムレベルでプロトタイプし、ノイズや電力変動などの外乱によるシステムの性能への影響を分析する。

4.2 統合シミュレーション環境

4.2.1 システムの概要

Figure 4.1は統合マルチレベル・シミュレーション環境 (Integrated Simulation Environment; ISE) の概要を図示している。電力供給ならびに信号伝送のためのトランスポンダとリーダのAFE³回路間における電磁的な相互作用はアナログ/ミックスドシグナル (Analog/Mixed-Signal; AMS) シミュレーション言語である Verilog-AMS[97] にて記述しており、商用 AMS シミュレータの Harmony によりシミュレーションを実施する。一方、TS-CDMA⁴に基づいた衝突防止アルゴリズムを実現する DBE⁵は、カスタムソフトウェア・シミュレータを用いてビヘイビアモデル化した。シミュレータはC⁺⁺言語を用いて実装され、その詳細については3.3節で説明した通りである。さらに、AMS シミュレータとカスタムソフトウェアを接続するためのインタフェース・プログラムを、IEEE-1364 で標準化されている Verilog のプログラム言語インタフェース (Program Language Interface; PLI) 機能 [98] を用いて C++ 言語で開発した。システム全体は Microsoft Windows 上の .NET Framework 2.0 環境と Harmony が相補的に動作する。Verilog-AMS 単体によるシミュレータと較べると、カスタム・シミュレータとの併用はアルゴリズムの工夫によってシミュレーション時間の削減が容易であり、メモリ管理の最適化を行うことでより大規模なシミュレーションを可能とする。フルソフトウェアによるシミュレータと比較すると、シミュレーションの実行速度が低下する欠点があるが、逆により高精度かつ回路設計に即した評価結果を求められるという重要な利点が存在する。

ISE は超多重 RFID における通信システムの設計において不可欠な設計環境である。これは、ISE は様々な外乱のもとでの多重通信の性能をシミュレートできるだけでなく、実際のハードウェア設計における検証手段を提供することができるからである。また、デジタル部をカスタムソ

³Analog Front-end

⁴Time Slotting-Code Division Multiple Access

⁵Digital Back-end

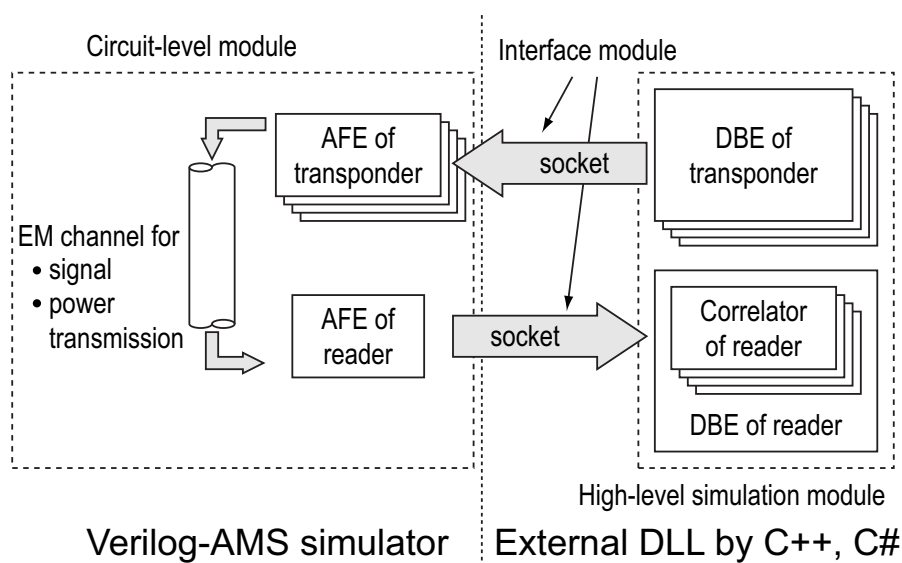


Figure 4.1: ISE の構造図

ソフトウェアで構成することにより、外乱のモデル化に対する柔軟性とシミュレーション性能を両立させることが可能である。ISE はアナデジ双方を同時にモデル化するため、ソフトウェア単体のシミュレータと較べるとノイズなど外乱のモデル化を高い精度でかつ柔軟に行うことができる。さらに、アルゴリズムレベルで処理を最適化することによりシミュレーションに必要とする CPU⁶ 時間やメモリ容量を軽減することができる。

ISE におけるデータフローを Figure 4.2 に図示する。トランスポンダとリーダはともに、機能に基づいて アナログ部 (AFE) および デジタル部 (DBE) に分けられている。また、トランスポンダ群とリーダ間における電力と信号の電磁的な伝送を取り込む通信チャネルのモデルは AFE 部に置かれている。AFE 部は回路レベルで、また DBE はシステムレベルで記述されているため、ミックスレベルによるシミュレーションが可能である。Figure 4.2 の下部に示されている AFE モジュールが図の中間に描かれている DBE モジュールと PLI によるインタフェースを通して接続されている。さらに、主制御モジュールが RFID システムの信号チェーンに沿って ID の伝送を取り扱い、誤り率を評価する。また、ID と CRC⁷ 符号を生成して DBE 部のトランスポンダ側に引き渡したのち、逆にリーダ

⁶Central Processor Unit

⁷Cyclic Redundancy Check (巡回冗長検査)

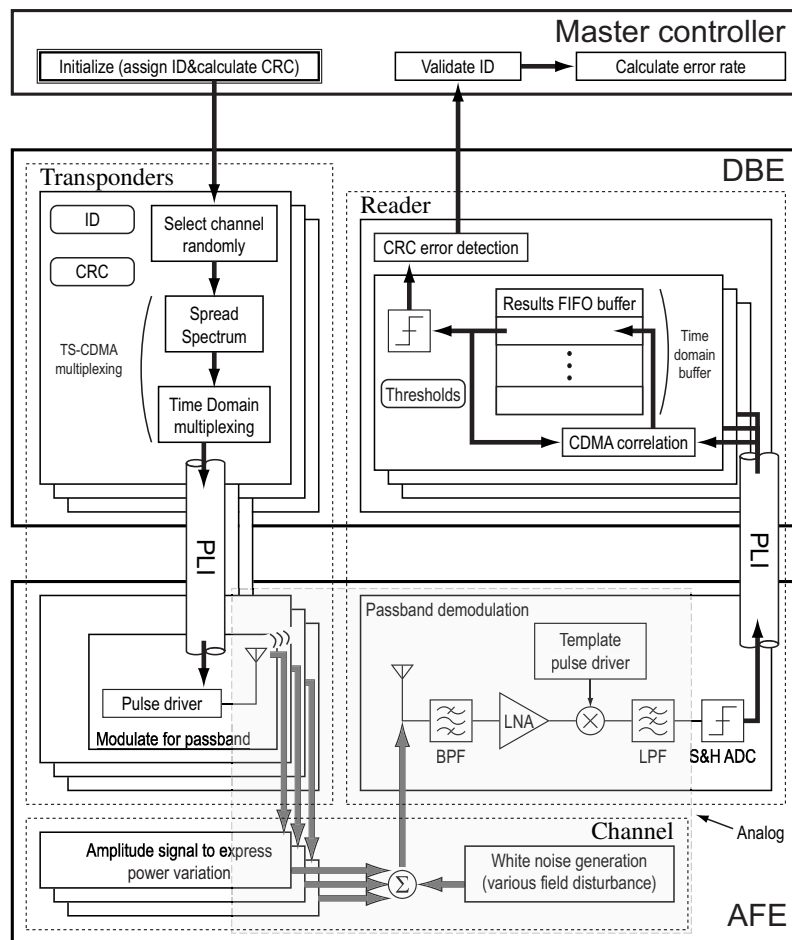


Figure 4.2: ISE のデータフロー図

側から逆拡散した結果を集めてその正当性を検証する。

4.2.2 AFE モジュールの回路レベル記述

トランスポンダは Figure 4.2 に示されるように、AFE 部が DBE 部から ID ビット列の拡散済み信号を受け取る。続いて、信号はインパルス列として変調され、仮想的にアンテナから輻射される。ここで、空中でのインパルスの伝送および全トランスポンダの応答の合成は通信チャネル内にモデル化されており、そこでは白色ノイズのような外乱の注入や信号電力の変動が同時に行われる。このとき、ID の伝送は断続的に行われるので、たとえリーダとトランスポンダ間の結合強度が時間軸上あるいは

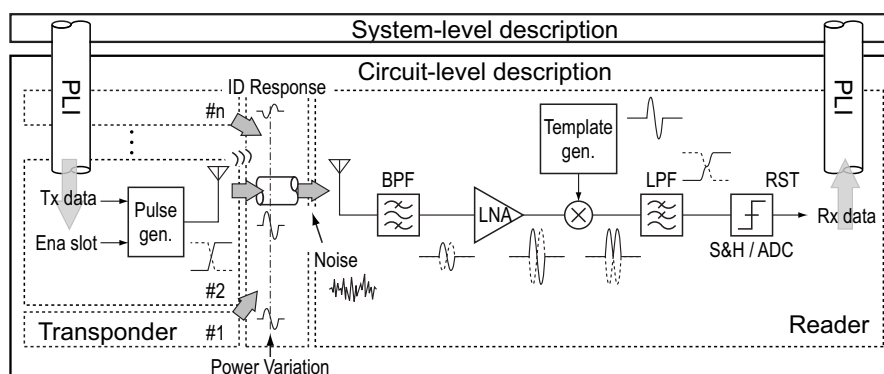


Figure 4.3: AFE 部信号フローの拡大図

両者の位置によって変動したとしても、トランスポンダは送信動作にない間は信号の輻射にかかる電力を節減しつつ、リーダからの電力波を整流してチャージすることができる。したがって、その動作電力は必要十分にチャージされていることと想定する。これにより、チャンネルモデルはトランスポンダからリーダへの一方向のみランダムに信号電力の強度を変動させる。リーダにおいては、AFE 部はチャンネルから信号を受け取り、バイナリデータを抽出して DBE 部に転送する。

信号の流れをより明確にするため、AFE 部だけを拡大して Figure 4.3 に示す。AFE 部は複数のトランスポンダ AFE とそれぞれ単一の通信チャンネルおよびリーダ AFE から成る。通信チャンネルはトランスポンダの出力をすべて集めて足し合わせ、そこに電力変動とノイズ注入を行う。

4.2.3 DBE モジュールのシステムレベル記述

トランスポンダの DBE 部は、主制御モジュールにより起動されて一意の ID 番号とその CRC 符号を与えられる。DBE 部のそれぞれのユニットは並行に動作するトランスポンダに対応づけることができ、TS-CDMA 通信プロトコルに従い ID 値を多重化して AFE 部に信号を伝送する。トランスポンダは CDMA⁸ チャンネルと TDMA⁹ スロットをランダムに選ぶとともに、リーダから電力供給されている限り ID データの拡散信号を再送する。一方、リーダの DBE 部は AFE 部からの信号をスロットバッファから抽出、CDMA に基づいた相関演算、および CRC 検証を経て逆拡散す

⁸Code Division Multiple Access

⁹Time Division Multiple Access

る。CDMA 関連における閾値 n_{th} は通信の誤り率を決する重要な設計パラメータのうちの一つである。CDMA 関連器からの出力が n_{th} よりも低ければ、相関結果は破棄される。ここで、 n_{th} を超える相関結果において TS-CDMA の確率的過程において誤って作りだされた、すなわちスロットと拡散符号が偶然一致した複数のトランスポンダの合成 ID 値を表すことがあることに留意されたい。その合成 ID は主制御モジュールの ID データベースには存在しないため、これをゴースト ID として取り扱う。

4.2.4 動作シーケンス

より詳しく ISE の動作を説明するため、シミュレーションのシーケンスについて記す。まず、ISE は Harmony により起動されて高位シミュレーションモジュールおよびインタフェースモジュールの動的リンクライブラリ (Dynamic Linkage Library; DLL) と接続する。ISE が起動すると、シミュレーションパラメータの設定が GUI¹⁰を介して行われる。必要な初期化を行った後、シミュレーションが開始される。トランスポンダは初期化フェーズ中に ID がランダムに割り当てられ、再送が終わって再び初期化されるまでその ID が保持される。Figure 4.4に ISE の動作シーケンス図を示す。シーケンスの概要は下記のとおり:

- (1) シミュレータの初期化が行われる。シミュレーションパラメータの設定画面を表示し、パラメータに基づいてトランスポンダとリーダが仮想的に用意される。トランスポンダは初期化フェーズにおいて ID がランダムに割り当てられる。
- (2) トランスポンダ群が仮想的にリーダの識別範囲に入る。現実のシステムでは、このときリーダから電力供給が行われてトランスポンダが動作し始める。トランスポンダの位置がランダムに求められ、動作開始タイミングと送信電力が導出される。
- (3) リーダが同期タイミングを知らせるために、実際のシステムでは電力供給波を 180 度反転する。高速化のため、ISE では同期プロセスを考慮しない。
また、トランスポンダはランダム機構によって通信チャネルを割り当て、ID 値を CDMA 拡散する符号を求め、送出準備を行う。
- (4) トランスポンダは DBE が拡散した ID 値を PLI を経由して AFE に引き渡し、これを自ら割り当てた TDMA チャネルを用いてインパ

¹⁰Graphical User-Interface

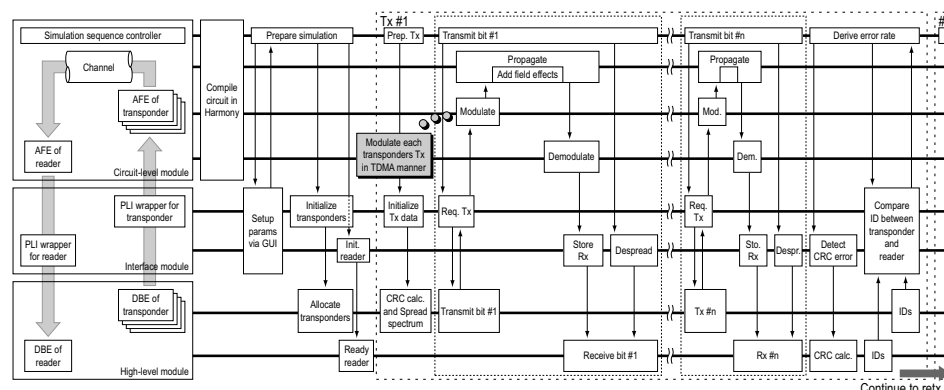


Figure 4.4: ISE の動作シーケンス図

ルス変調しつつ送出する。

- (5) Harmony の内部でトランスポンダの送出 ID が多重化され疑似チャネルを伝搬する。この際、ノイズなど外乱が加えられる。
- (6) チャネルを通過した信号はリーダの AFE で復調されデジタイズされる。結果は PLI を経由してリーダの DBE に引き渡される。
- (7) リーダは受け取った信号を相関器にて逆拡散する。このとき、相関器の閾値に満たない逆拡散値や CRC が合致しない ID は破棄される。
- (8) リーダの受け取った ID とトランスポンダの送出した ID が一致していることを PLI 経由で確認し、エラーを確定する。
- (9) 再送する: (3)–(8) を繰り返すたびにエラー検出を行う。

最終的にリーダが受信した ID は、トランスポンダに照会されて実際に送出された ID と等しいことを確認する。ここで、ID の生成ならびにゴースト検出は主制御モジュールとして Verilog-AMS により動作記述されている。

4.2.5 ISE の実装に伴う課題

Verilog-AMS によって行われる回路レベルや動作記述レベルのシミュレーションは内部的に SPICE 記述に展開されて実施される。このことは、モジュール間のあらゆる配線やその内部で使用する変数が SPICE によりモニタされることを意味し、このため AMS シミュレータモデルは非常に大きなメモリ容量を必要とする。たとえば、AFE 部に 1,000 個のトラ

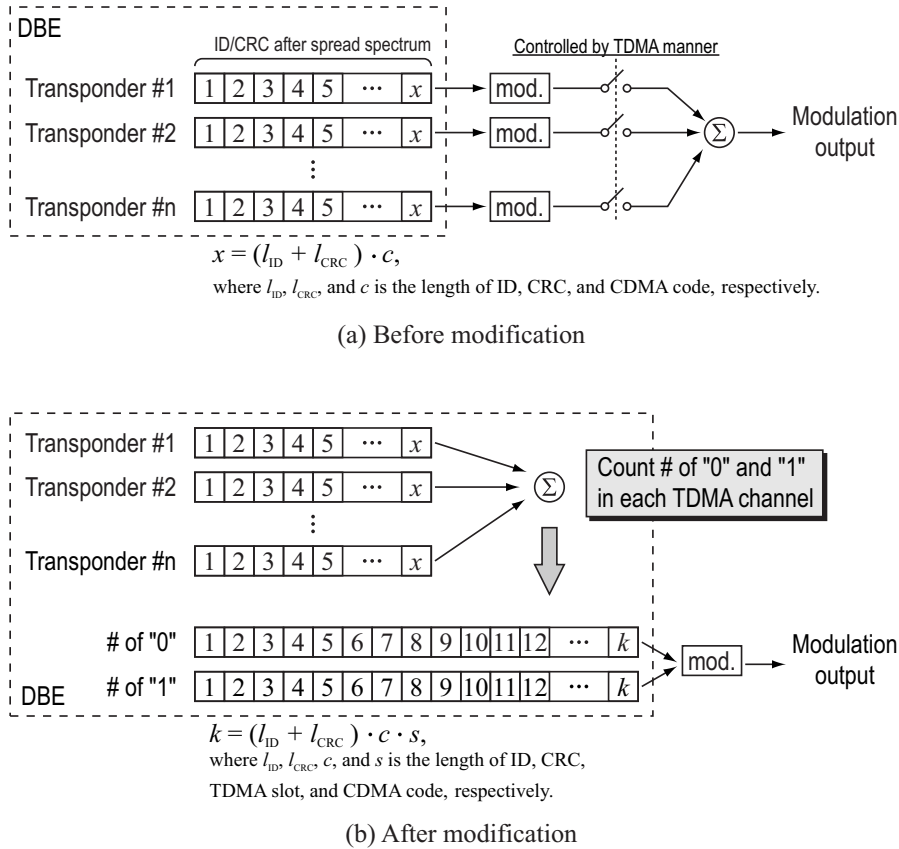


Figure 4.5: 実装において直面した問題に対するモデルの修正

ンスポンダ・ユニットを内蔵すると、それだけで1 GBを超えるメモリを必要としDBE部の拡散／逆拡散処理に要求されるメモリ量と合わせると4 GBを超過するため、一般的なコンピュータではシミュレーションが正常に実行できない。そこで、Figure 4.5に示すようにAFE部のトランスポンダ・ユニットでの変調処理を再構成した。個々のトランスポンダに対して固有の変調器を用意するのではなく、全てのトランスポンダ出力をデジタル領域であらかじめ多重化しておき、その結果得られる合成信号を一つの変調器で一次変調する。これによってモジュール間の相互配線数を大幅に削減でき、AFE部の要求メモリ量を100 MB以下に抑えることができる。

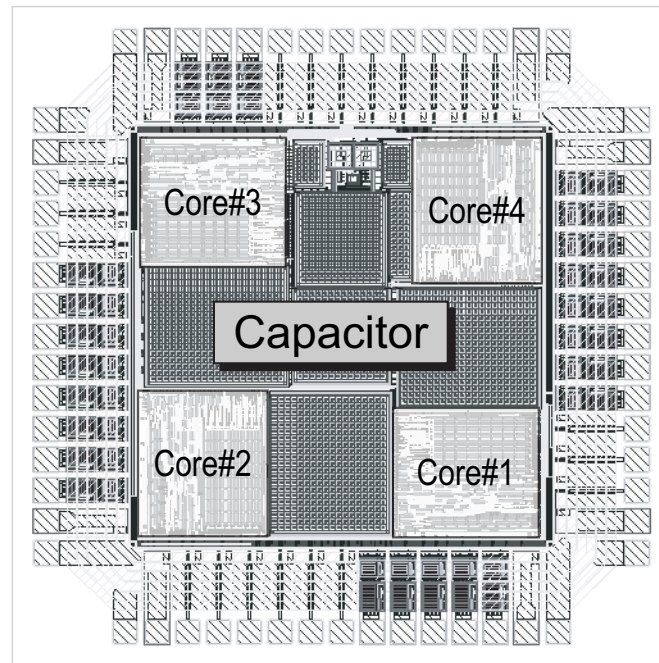


Figure 4.6: ISE の援用による設計チップのレイアウト

4.2.6 ISE 援用によるチップ設計

ISE はハードウェアの設計結果を Verilog-AMS あるいは SPICE モデルとして取り込むことができる。これにより、アナデジ混載である RFID システムの現実に即した評価ならびに検証が可能である。そこで、3章で設計したチップに対して ISE を適用することによって AFE と DBE の設計を改良し、トランスポンダチップを実装した。Figure 4.6 に設計したチップのレイアウトを示す。多重通信の評価試験に用いることができるように、本チップには4つのトランスポンダコアが実装されており、チップ単体でも4多重の RFID 通信を評価することが可能である。また、チップを複数用いることによってさらに多くの輻輳状態を実現することもできる。本チップの設計データを Table 4.1 に示す。

4.2.6.1 ISE とチップ設計との相関

ISE の AFE 部は Verilog-AMS を用いて動作記述レベルでモデル化されているが、このモデルは実装チップの回路モジュールと 1 対 1 に対応す

Table 4.1: トランスポンダチップの設計諸元

	Layout
Process	0.35 μm CMOS@3.3 V
# of transistor	10,697 $\times$ 4
Digital back-end	210,300 $\mu\text{m}^2 \times 4$
Analog front-end	34,863 μm^2

る。このため、ISE では必要に応じて動作記述モジュールを設計回路より抽出したネットリストと差し換えることにより、ハードウェア設計の検証や評価に用いることが可能である。このビヘイビアモデルと実際の回路との相関をとるため、シミュレーションにより変調波形を取得した。AMS シミュレータによる AFE 部のシミュレーション結果を Figure 4.7 に示す。(a) に示されている最初の 8 本の波形は 4 つのトランスポンダから与えられた拡散後の ID データのデジタルパルスならびに変調インパルスであり、続く波形はチャネル伝搬中に観測されるインパルスを示す。このインパルスをリーダで復調、およびデジタイズしたものが (a) の下部に示されている。4 つのトランスポンダはリーダから異なる距離にあるものと想定し、すなわちそれぞれの結合係数と出力信号レベルはその距離によって異なる値に設定されている。チャネル伝搬信号は各トランスポンダの出力が合成されるため、個々のインパルスの信号レベルに変動が見られる。これと比較するため、ISE とそれぞれのトランスポンダが全く同じ ID データと結合レベルであると仮定したときの SPICE によるシミュレーション結果が (b) に示されている。これは 4.2.6 節において説明したトランスポンダチップのレイアウトからネットリストを抽出して取得したものであり、ISE は動作記述レベルのモデルであるにも関わらず、実際のレイアウトから得たトランジスタレベルによるシミュレーション結果と強い相関を持つことが明らかである。これらの評価を通じて、ISE によるシミュレーションを用いた設計結果と密接に連携して検証および評価手段は、アナデジ混載のシステムにおける有効な設計手法であることを実証した。

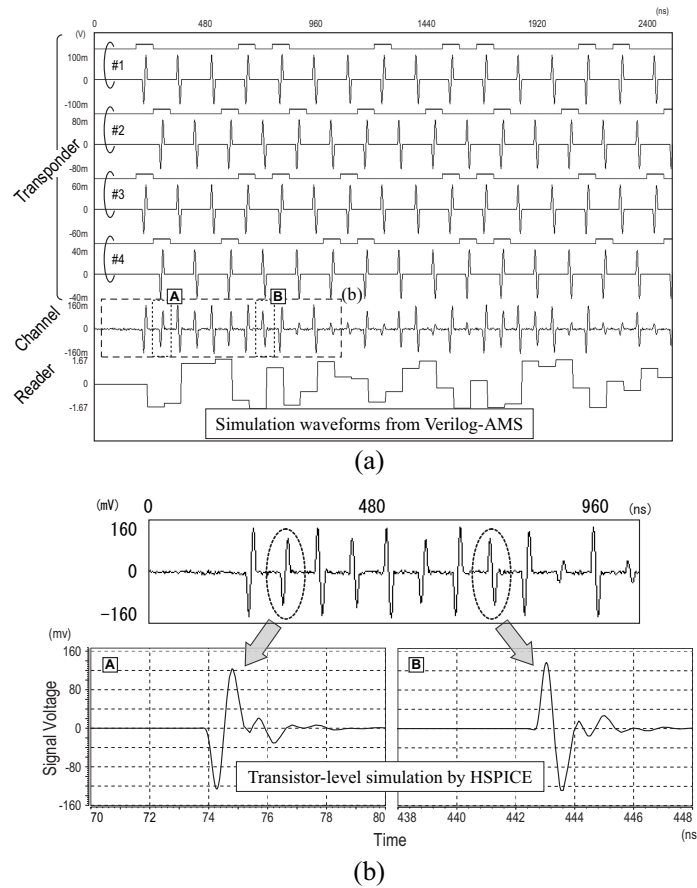


Figure 4.7: AFE 部のシミュレーション結果: (a) ISE により取得した波形、(b) ISE の拡大波形とそれに対応するトランジスタレベルの波形

4.2.7 他の従来モデルとの比較

4.2.7.1 モデルの記述スタイル

1,000 を超える ID タグの多重通信の実現可能性を評価するため、これまで4つの異なる方法で超多重RFIDシステムのモデル化を行ってきた。すなわち、数値モデル、ハードウェア・エミュレータ、フルソフトウェア・シミュレータ、そしてミックストレベル・シミュレータである。それぞれについて以下にまとめる。

数値モデル 数値モデルは、トランスポンダがランダムでチャンネルを選ぶ際の確率的な分析による衝突確率を立式したものである。このモデル

では誤り率の理論的な最小限界を示すことができるが、回路動作を反映するための現実的な外乱や擾乱を含めることはできない。

ハードウェア・エミュレータ 3.2節に説明したように、RFID システムのハードウェア・エミュレータはFPGA を用いて構築された。このモデルはシステム全体を効率的に築き上げ、並列動作によってトランスポンダとリーダのペアによる 1,000 を超えるサブモデルをもって通信性能を高速に取得することができる。外乱については、その物理的な性質をデジタル表現による論理合成で等価的にモデル化できる限りにおいてモデルに組み入れることが可能である。

フルソフトウェア・シミュレータ 3.3節で議論したように、カスタムソフトウェアは RFID システムモデルに対して様々な性質の外乱を柔軟に組み込むことができるため、RFID 通信のロバスト性を評価することができる。システム性能の取得効率は最も高くなるが、アナログの信号表現は時間領域・周波数領域のいずれにおいても取り扱いが困難であり、よって回路レベルの動作検証と組み合わせる必要がある。

ISE ISE は回路レベル記述とシステムレベル記述が協調する。これによりアナログ／デジタル双方においてシステム全体の評価が可能である。カスタムソフトウェアによる高位モデル化手法と組み合わせ連携させることにより、システムレベルの性能と一次変調や電磁結合のような回路レベルの動作を同時に得ることができる。

4.2.7.2 モデル比較

各モデルによる IDER¹¹の比較を Figure 4.8に示す。また、Table 4.2に IDER を導出する際に用いたパラメータセットをまとめる。ここで、数理モデル以外のモデルで IDER の導出にかかった実行時間を Table 4.3にまとめる。このとき、シミュレーションの実行環境は Microsoft Windows XP で動作中の SUN Fire X2100 M2 ワークステーションである。このワークステーションの主な仕様としては、CPU がデュアルコアの Opteron 1218 であり、メモリが 4 GB@PC2-5300 である。このとき、モデルによる衝突率の本質的な相違を求めるために環境ノイズや電力変動のような外乱は注入されていない。全モデルにわたって IDER は再送数が増加するに

¹¹ID Error Rate

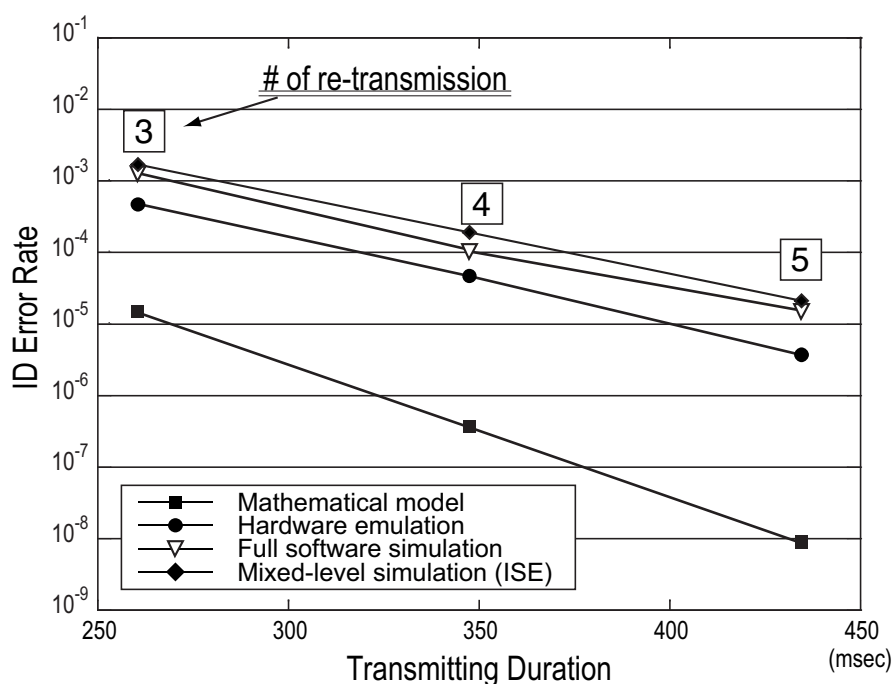


Figure 4.8: モデルによる IDER の比較

Table 4.2: モデル比較に用いたパラメータセット

r :	# of CDMA ch.	16
x :	# of TDMA ch.	512
n :	# of transponders	1,000

つれて改善している。ISE による IDER はフルソフトウェアによる IDER よりも若干劣化している。DBE 部はフルソフトウェア・シミュレータを部分的に利用しているため、この IDER の劣化は AFE 部、つまりは一次変調および電磁伝搬によって生じたものと考察される。理想度の相違によってモデルの示す IDER に差異が見られるが、4.2.6.1 節に示したとおり、ISE は実際のハードウェア設計に対して高い相関を持っているので、Figure 4.8 においては、ISE によって算出された IDER が最も実用状態に近い値である。

Table 4.3: 認識を1,000回繰り返したときのシミュレーション時間の比較

FPGA ハードウェア・エミュレータ	(分) 1' 26" (秒) (1.00)
フルソフトウェア・シミュレータ	22' 09" (15.45)
統合シミュレータ環境	114' 51" (80.13)

Table 4.4: 性能評価に用いたパラメータセット

r : # of CDMA ch.	64
x : # of TDMA ch.	64
n : # of transponders	1,000

4.3 1,000を超えるRFIDシステムのプロトタイプ

本節では Table 4.4にまとめたパラメータを用いて ISE により求められた性能に関する分析を示す。

4.3.1 チャネルノイズの影響

RFID システム全体の分析例として、1,000 多重 RFID システムを ISE でプロトタイプ化することにより IDER を求めた。Figure 4.9 には SNR¹² と IDER の間の関係が描かれている。20 dB までの環境ノイズの影響が求められており、ノイズがない場合と比較されている。電力変動はこのシミュレーションでも考慮されていない。ISE はノイズの小さい環境ではフルソフトウェア・シミュレータと類似した IDER を示す一方、通信チャネルのノイズ電力が大きくなるとその差が拡大することが示されており、非常に興味深い結果となっている。

この結果は環境ノイズの取り扱いにおける差異に基づく。概念図を Figure 4.10 に示す。ISE はノイズをアナログ変数として自然に包含することができるが、ソフトウェア・シミュレータはノイズの影響を完全にデジタルで近似するからである。そのため、ISE を用いることによって、環境ノイズの影響を考慮しながら RFID システムの設計パラメータを最適化す

¹²Signal-to-Noise Ratio (信号対ノイズ比)

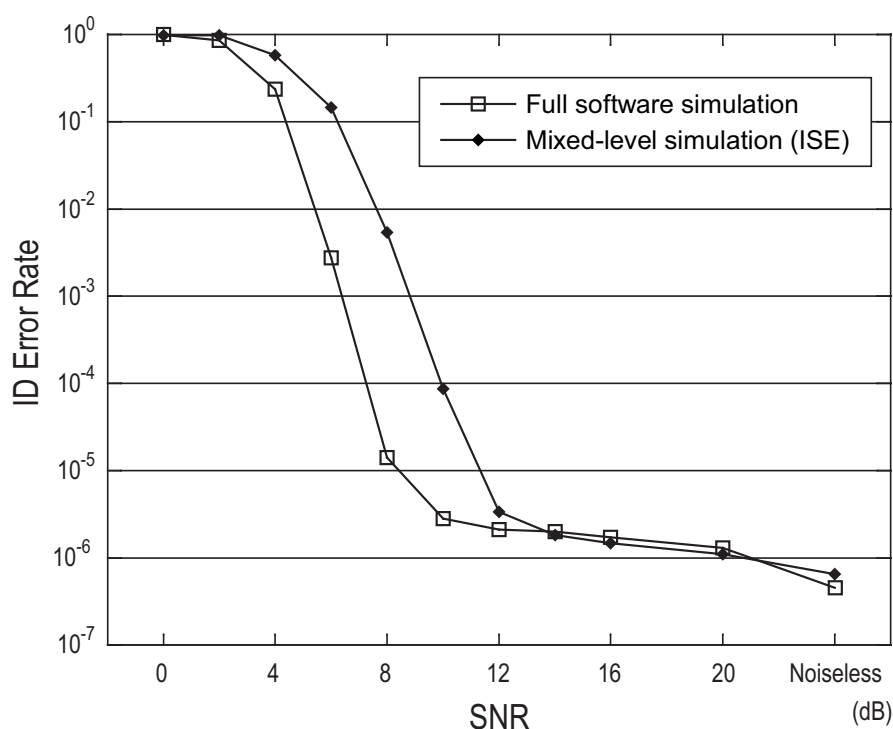


Figure 4.9: 環境ノイズと IDER の関係

ることができることが明らかにしたと言える。さらに、Verilog-AMS における AFE の構造的な記述によって、この結果はトランジスタレベルの設計にすぐに移行することができる。これはフルソフトウェアによるアプローチでは実現できない重要な特徴である。ここで、IDER がノイズのない環境においてもゼロにならないのは通信方式が確率的手法による衝突防止アルゴリズム [79] を用いているからである。

4.3.2 信号電力の変動による影響

信号電力強度の変動を想定するときの IDER、ならびに NGID¹³を Figure 4.11 に示す。電力変動とは相対的な位置関係や障害の存在によるトランスポンダとリーダの間で起きる電磁結合の強さの変化と等価である。図は左端の 2 点が電力変動を考慮しない場合であり、そのうちの左側は比較のためソフトウェア・シミュレータを用いて導き出したものである。一

¹³# of Ghost IDs (ゴースト ID 数)

	Slot #1	#2	#3	Totally digitized
Transmitted	-1	+1	+1	
Noise	0.187	0.231	-0.069	
Received	-0.813	1.231	0.931	

(a)

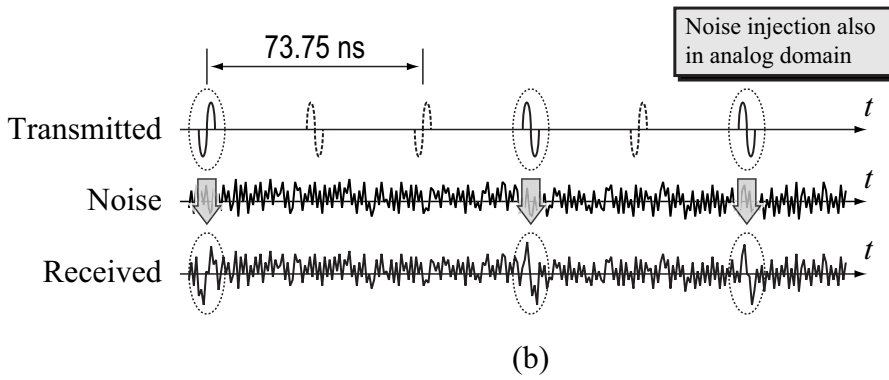


Figure 4.10: 信号とノイズの取り扱いにおける差異: (a) ソフトウェア・シミュレータ、(b) ISE

方、残る右側3点が変動を考慮する場合の結果である。

図に示されるように、SNRが18 dBであるからトランスポンダの応答はノイズの影響をほとんど受けず、ソフトウェア・シミュレータとISEの結果に大きな差異はない。そのため閾値が0.8でもIDERの劣化は小さい。ところが、電力変動を考慮した場合のISEのシミュレーション結果によれば、このときIDERが大きく劣化することがわかる。これは、トランスポンダとリーダの距離に応じて結合強度が変化し、トランスポンダの信号電力が弱められると、積和演算により行われる符号相関により得られる相関値も低くなってしまうためである。このことを立式すると、たとえば受信ビット列を $\mathbf{R} = \{r_0, r_1, \dots, r_n\}$ 、拡散符号を $\mathbf{S} = \{s_0, s_1, \dots, s_n\}$ とおくと、 $\mathbf{R}$ と $\mathbf{S}$ の相関値は

$$\mathbf{C} = \{c_0, c_1, \dots, c_n\} = \sum_k (r_k \cdot s_k)$$

である。このとき、仮に受信ビット列が電力変動により x 倍されたとす

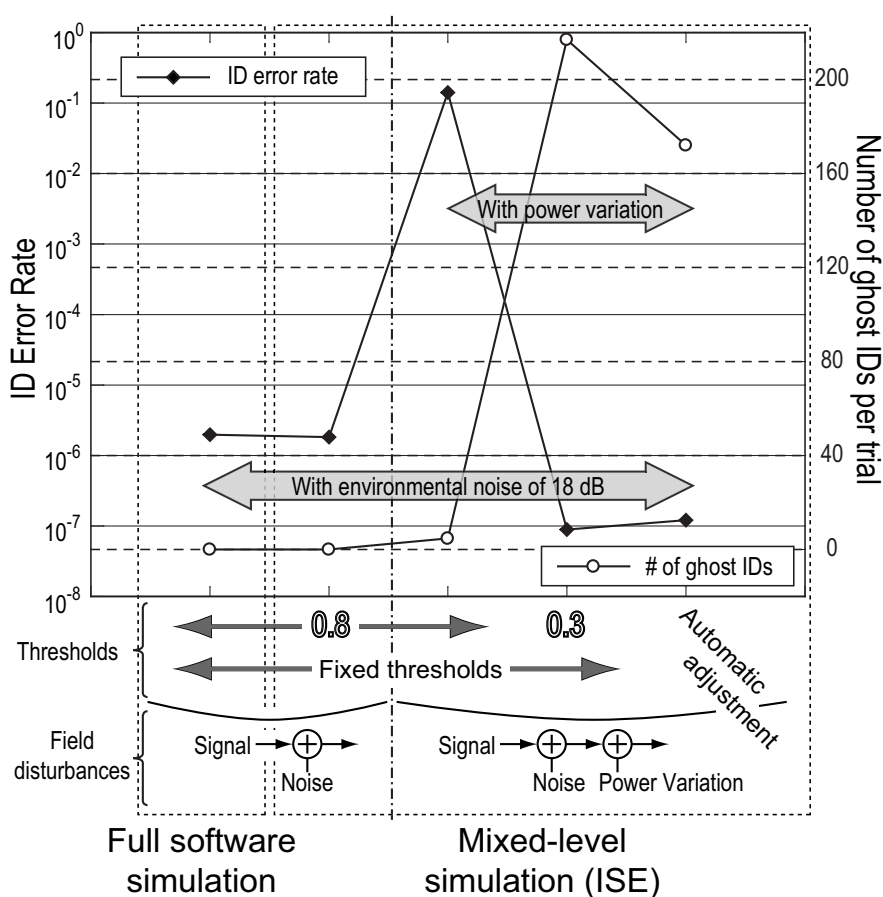


Figure 4.11: 閾値の選定と IDER/NGID の関係

る。ただし $0 \leq x \leq 1$ である。このときの相関値は

$$C_x = x \sum_k (r_k \cdot s_k)$$

である。これにより、相関値もまた電力変動の影響を大きく受けることが明らかにした。ここで、閾値を 0.8 に設定すると電力変動による相関値の劣化が閾値の変動許容幅を大きく超えるため、正常な拡散データに対してさえ相関器が反応できない。

これに対して、閾値を 0.3 に設定すると相関器の反応感度を高めることができ、通信時間内に ID を取得できないトランスポンダ数が低減できることが図から読み取れる。しかるに、本来は相関が取れるべきでないノイズ成分に対しても、相関器が敏感に反応して逆拡散してしまう。誤っ

て逆拡散されたデータの大部分はCRC符号による誤り検出によって排除されるが、一部は2.3.5.1節で説明したように排除されることなく誤り検出処理を通過してしまう。Figure 4.11において閾値が下げられると同時にゴーストIDが急増しているのは、このことが原因である。

そこで、ISEでは低閾値のIDERを保ったままNGIDを削減するために、自動的に閾値を調整する機構を組み込んだ。図において最も右端の点は自動調整を有効にしたときのIDERならびにNGIDを表している。これによると、IDERにほとんど変化がないにも関わらずNGIDに減少傾向が見られる。ここで、自動調整機構はIDビット系列の最初の10 bitを逆拡散する間だけ相関結果に応じて閾値を動的に変更する。すなわち、この機構による調整が有効な期間 T_{ATA} は拡散符号長を l_c 、スロット数を l_t とおくとき、以下のように表される。

$$T_{ATA} = \frac{1}{13.56 \text{ MHz}} \cdot (10 \times l_c \times l_t)$$

この機構は最初の10 bitの調整有効期間 T_{ATA} においてのみ相関値に応じて閾値を徐々に下げる。この期間 T_{ATA} が終了すると調整された閾値を保持し変更しない。今回のシミュレーションでは調整期間を10 bitに固定し、調整方法を単純デクリメントとしたが、この期間や方法についてより深く分析することでNGIDに対するさらなる最適化が可能であると考えられる。

4.4 結言

本章では、提案した通信方式のアナログ領域を含めた全システムについて性能評価するために、3章で提案したカスタムソフトウェアによる高位モデルとVerilog-AMSによる回路レベルモデルが協調動作する統合マルチレベルシミュレーション環境を提案した。ISEは協調的にアナログ混在で一次変復調ならびに多重化の両方の側面から評価を可能とすると同時に、ハードウェア設計と並行して設計結果を本検証系に組み入れることが可能である。一方、DBEはソフトウェアにより実現されており、このことは外乱モデルに対する柔軟性やシミュレーション速度の最適化といった面で有利に働く。ノイズのあるチャンネルにおける通信の評価を通して3章のシミュレータと比較した。シミュレータはデジタル領域でノイズを注入するため、アナログとして注入するISEよりもノイズの影響が小さく現れることが判明した。特に低SNRで傾向が顕著になることがはっ

きりした。また、送信信号の電力変動を外乱要因として与え、このもとにおける閾値と誤り率の関係を再検討した。この結果、電力変動によって誤り率が激増すること、またその誤りは閾値を下げることで削減できること、その一方で NGID が増加することが明らかとなった。閾値の調整機構を試行的に実装したところ、NGID の削減に効果があることが示された。

統合シミュレーション環境を用いることで、従来は回路モデルとビヘイビアモデルを併用しつつ進める必要があった多重通信システムの動作検証や性能見積もりを、設計と並行して包括的に実施することができるようになった。これにより、アナデジ混載のミックスシグナル Systems-on-a-Chip (SoC) の設計におけるトップダウン・アプローチの有効性を実証した。

第5章

結論

物流や流通分野でバーコードの置き換えとして期待される RFID¹のパッシブ・トランスポンダにおいては、消費電力や回路面積を低く抑えつつ、高速な識別情報の読み取りを可能とする通信方式が希求されている。本研究の目標はチップ面積を最小限に抑えつつ非常に高い識別効率を提供できる RFID システムを開発することにある。識別効率の高い RFID システムを設計するためには確率的手法に基づく衝突防止アルゴリズムと、それを実装する通信方式を実証するためのプロトタイプシステムの構築が不可欠である。本研究は 400 ms に 1,000 個の識別を可能とする衝突防止アルゴリズムと、それを実装するための RFID 向け通信方式および回路方式を提案し、さらに多重通信や外乱の影響を評価することができる高位モデルを構築した。これにより、超多重 RFID システムのバックエンドならびにアナデジ混載チップの設計手法を確立した。

1章では研究の概要について説明した。現在の個体識別システムにおけるトレンドと課題について紹介し、RFID 技術が非常に大きな注目を浴びていることを述べた。続いて、RFID 技術を物品識別へ応用する際に解決されるべき問題としてトランスポンダ応答の衝突をピックアップし、3種類に分類できることを説明した。特に問題となる複数トランスポンダと単一リーダの間における衝突について決定的手法と確率的手法に分けられることを述べ、その従来技術についてまとめた。2章では物流や流通分野への適用を視野に入れ、確率的手法に基づく認識効率の非常に高い RFID 向け衝突防止アルゴリズムを提案し、それに基づく通信方式ならびに回路方式について導出した。3章では、多重通信の性能評価のために高位モデルとして構築したハードウェア・エミュレータならびにソフトウェア・シミュレータによるバックエンド回路の設計手法を提案し、DBE²の設計にあたって重要となる多重パラメータの現実 に即した最適解を導出した。4章では、3章で提案したソフトウェア・シミュレータを AMS³商用

¹Radio Frequency Identification

²Digital Back-end

³Analog/Mixed-Signal

シミュレータと統合することによって電力変動やチャネルノイズといったアナログ領域における外乱の影響を可能にし、アナデジ混載チップの設計手法を明らかにした。各章での研究内容を以下にまとめる。

2章では、物品の識別を高速に行うことを意図する衝突防止アルゴリズムを考案した。このアルゴリズムはTS-CDMA⁴多重化、CRC⁵符号による誤り検出、再送による誤り回復から構成される。TS-CDMAはDS-CDMA⁶とTDMA⁷の組み合わせることによって、従来のFramed ALOHAやFTDMAよりも高い多重度を可能とする多重通信方式である。物流や流通への応用を考えたときにトランスポンダは電池を内蔵しないパッシブ方式が望ましいため、その回路構成はできるだけ簡略化する必要がある。本アルゴリズムは確率的手法に属しており、トランスポンダがPRSG⁸を内蔵することによって、チャネル割り当てをランダムプロセスに基づいて自発的に行うことによって、決定的手法で必要となるトランスポンダへの指令を排除し、実装の際の面積削減を図った。次に、本アルゴリズムを実現する通信方式を提案した。このとき、リーダからトランスポンダへ送信されるダウンリンク通信については電力供給と時間枠・スロットの同期のみが与えられればよい。電力は誘導結合により供給し、同期タイミングの通知は送信時間枠のはじめに電力波を1パルス期間のみ反転させることで通知するとした。それにより、トランスポンダから指令を受信するための復調回路を排除した。一方、アップリンク通信としては、先の衝突防止アルゴリズムに加えて一次変調としてインパルス変調を選定した。これは従来の負荷変調を用いるとき、1,000を超えるトランスポンダが識別領域に存在する超多重状態ではインピーダンスの整合が取れないためである。変調はUWB-IR⁹に基づいてインパルスをbi-phase変調とpulse position変調の組み合わせで輻射して行うBP³¹⁰変調を提案した。この変調によってパルスの位置と位相の双方で情報ビットが判断することにより、本変調方式では高いロバスト性とリーダのトラッキング処理の排除を達成した。一方、提案手法は衝突防止アルゴリズムがランダムプロセスに基づくため、衝突確率を完全にゼロにすることはできない。そのため衝突により発生する誤りについてCRC符号と再送によっ

⁴Time Slotting-Code Division Multiple Access

⁵Cyclic Redundancy Check (巡回冗長検査)

⁶Direct Sequence-Code Division Multiple Access

⁷Time Division Multiple Access

⁸Pseudo Random Sequence Generator (疑似乱数生成器)

⁹Ultra Wideband-Impulse Radio

¹⁰Bi-Phase Pulse Position

て対応する。再送による衝突の再発生を軽減するため、トランスポンダがリーダと同期を取って送信時間枠がはじまると、トランスポンダはチャネルをランダムで再び選択しなおす。この衝突防止アルゴリズムに対して数理的な分析を与え通信パラメータを導出した。その結果、理論的な誤り率は 2.52×10^{-9} と与えられ、実用に問題のない通信方式であることを実証した。

続いて、通信方式を実現するための回路方式を提案した。トランスポンダ／リーダともにアナログ領域で変復調を司る AFE¹¹とデジタル領域で多重通信を司る DBE から構成される。それぞれの回路において重要な役割を果たす構成要素について項目別に説明した。また提案した回路方式において AFE の性能を確認するため回路レベル記述によってシミュレーションを実施した。これにより、一次変復調回路の動作が確認できた。通信方式の基礎となる機能の実証実験としてトランスポンダのテストチップを試作して動作検証を行った。チップの出力から TS-CDMA 多重化とインパルス変調双方において設計が正しいことが確かめられた。

3章では、提案した通信方式をバックエンド設計の側面から検証するための手法として2種類の高位モデル化による評価システムを提案した。2章における多重通信の評価は理論分析に基づくものであるため、現実的な状況とは乖離するところがある。そこで、特に重要となる信号伝搬の劣化要因について分析し、この劣化要因を調査するための環境として高位モデルを位置づけた。評価システムの1つはFPGA¹²によるハードウェア・エミュレータである。トランスポンダとリーダのDBEをFPGAボードに実装し、両者をデジタルで接続することでTS-CDMAとCRC、再送から構成される衝突防止アルゴリズムの基礎評価を可能とする評価系である。エミュレータを用いた評価によって再送による衝突率への効果が確かめられた。特に、ここではTDMAチャネル数よりも再送数による衝突率に対する影響が大きいことが明らかにした。また、トランスポンダ／リーダの結合にデジタル的に白色ノイズを加え、リーダがCDMA¹³で拡散された信号を逆拡散するための相関器における閾値の制御がノイズへのロバスト性にどの程度影響するのかを明らかにした。一方で、閾値の制御はNGID¹⁴にも影響を与えることが明らかとなった。このため、通

¹¹Analog Front-end

¹²Field Programmable Gate Array

¹³Code Division Multiple Access

¹⁴# of Ghost IDs

信チャンネルの SNR¹⁵に応じて適切な閾値を見いだすことが重要であることがわかった。

もう1つの評価システムとしては、C#で実装されたカスタムソフトウェア・シミュレータである。シミュレーション時間はエミュレータのそれよりも大幅に増大するが、ソフトウェアの柔軟性によってトランスポンダ数や再送数の増減、チャンネル配分などパラメータを変化させることによる性能への影響、あるいは距離の変動や電力ばらつき、種々のノイズなど外乱によるさらに多くの誤り要因に対して考察することが可能となった。また、通信状況がリアルタイムに画面表示されるので、本シミュレータにより視覚的に誤りの傾向をつかむことが可能である。本評価系を用いて3つの通信性能に関する分析を行った。はじめにエミュレータで明らかになった再送数の衝突率への影響について、より詳しく調べるために環境ノイズが存在するチャンネルを想定してシミュレートした。その結果、ノイズによる影響は無視することができず、ノイズのない環境との乖離は再送数を増やすほど大きくなることが明らかとなった。また、TDMAチャンネルを増やして再送数を減らすとノイズの影響がより大きくなる傾向が見い出した。次に識別領域に存在するトランスポンダが1,000を超過する場合について誤り率性能の評価を行った。ここでもチャンネル数を減らして再送数を増やすほうがチャンネル容量に余裕が生じることが明らかにした。最後にロバスト性を評価するため、TS-CDMAにおけるTDMAとCDMAの配分について評価した。TDMAチャンネルを増やすとノイズへのロバスト性が劣化することがわかった。TDMAとCDMAの配分についてはハードウェア規模とノイズに対するロバスト性のトレードオフであるから、最適点を導出してそのパラメータをまとめた。

4章では、提案した通信方式のアナログ領域を含めた全システムについて性能評価するために3章で提案したカスタムソフトウェア・シミュレータをAMS商用シミュレータに組み込んだ統合マルチレベルシミュレーション環境を提案した。AFEのアナログ処理をAMSシミュレータ上の動作記述モデルが担当し、またDBEのデジタル処理をソフトウェアによる高位モデルが実行することで協調的にアナデジ混在で一次変復調ならびに多重化の両方の側面から評価が可能となった。AMSシミュレータはVerilog-AMSおよびSPICEによるモデル記述が可能であるため、ハードウェア設計と同時に検証系に組み入れることが可能である。一方、DBEはソフトウェアにより実現されており、このことは外乱モデルに対する

¹⁵Signal-to-Noise Ratio (信号対ノイズ比)

柔軟性やシミュレーション速度の最適化といった面で有利に働く。この構築した統合シミュレータについて2章および3章で導出した多重通信モデルと比較を行った。その結果、ここでも誤り率に対する再送による効果が高いことを明らかにした。理想化の程度によりモデル間の差異はあるものの、傾向として近いことを示し、よってこれらの高位モデル化によって現れる誤り率の違いを明らかにした。このとき、モデルを現実近づけるほど誤り率に劣化が見られ、外乱による影響に伴う様々な劣化要因をモデルに組み込む必要があることがわかった。同時に、これらの要因は適切な手法によってモデルに採り入れる必要があることを示した。このISE¹⁶を用いて1,000 多重システムの性能評価を2つ行った。第1にノイズの取り扱いによるソフトウェア・シミュレータの差異である。ソフトウェア・シミュレータはデジタル領域でノイズを注入するため、アナログとして注入するISEよりもノイズの影響が小さく現れることが判明した。特に低SNRで傾向が顕著になることがはっきりした。また新たに送信信号の電力変動を外乱要因として定義し、このもとでの閾値と誤り率の関係を再検討した。この結果、電力変動によって誤り率が激増すること、またその誤りは閾値を下げることで削減できること、その一方でNGIDが増加することが明らかとなった。閾値の調整機構を試行的に実装したところ、NGIDの削減に効果があることが証明された。

以上の研究成果により、超多重応答を可能とするRFIDシステムの通信を実現し、そのハードウェア設計手法を確立した。提案した方式は確率的に衝突を防止するため、ノイズのない状態はもちろんのこと現実に即したノイズのある状況、電力変動のある状況における衝突率を可能な限り下げる必要がある。このため、今後の課題としては以下の通りあげられる：

- (1) 誤り率の改善に向けてトランスポンダの効果的なミューティングを検討し、通信方式に採り入れる。
- (2) 通信チャンネルのSNRに応じた閾値調整手法を確立する。
- (3) 実証システムを試作し、その多重性能を証明する。

提案した衝突防止アルゴリズムはランダムプロセスに基づいて確率的に通信の衝突を防ぐ。そのため衝突確率をゼロにすることはできないが、これをゼロに可能な限り近しくするために有効な手段として考えられるのが、トランスポンダのミュートである。これはトランスポンダが一時的

¹⁶Integrated Simulation Environment (統合シミュレーション環境)

に応答しなくすることを意味する。ミュートするタイミングについては二つ考えることができる。第1に ACK¹⁷信号によるミュートである。本アルゴリズムにおいて、トランスポンダは正常に認識された後も電力が供給され続けている限り識別情報の再送を続ける。しかるに、一度正常に認識されたトランスポンダは、もはや応答する必要が全くない。このようなトランスポンダの存在は衝突率をあげ効率を低下させる。これを防ぐためには、リーダーが識別できたトランスポンダに ACK を送信して応答を禁止する必要がある。このためにはトランスポンダが同期パルスだけでなく、ACK を受けるための仕掛けが必要である。ACK は通常 ID を添付して送信されるため、ダウンリンクにも変復調が必要となり回路規模に影響する。また、ACK による通信時間への影響も大きい。そのため、この ACK によるミュートを行うには回路規模・消費電力と通信時間、ならびに認識率に関わるトレードオフを検討する必要がある。第2はランダムミュートである。すなわち、トランスポンダが内蔵する PRSG の出力によってミュートするかどうか決定する。これは同時に通信しようとする見掛けのトランスポンダ数を減少することで衝突率の削減に影響するとの考えに基づく。こちらは回路規模に大きな影響をおよぼさないが、ACK によるミュートよりも効果が少ないと考えられる。これらミュートを適用したときの性能への影響はソフトウェア・シミュレータあるいは ISE で評価可能である。

エミュレータおよび ISE を用いた評価を通して、ノイズや電力変動などの外乱による影響を考えるとリーダーの内蔵する相関器の閾値が IDER¹⁸や NGID といったシステム性能に大きく影響することがわかった。このことは、チャンネルの SNR に応じて適切な閾値を選ばなければならないことを意味する。そのためチャンネルの状態に応じて適宜、閾値を調整するための何らかの機構が必要と考えている。4章の評価で導入した閾値自動調整機構はその一例である。ノイズに対する効果は示されたが NGID についてはさらに改良が必要であることが明らかとなった。これもソフトウェア・シミュレータや ISE によって導出が期待できる。

3つめの課題として実証実験をあげる。4.2.6節において設計した多重通信の実験用チップは、現在試作中である。提案した通信方式や回路方式、導出パラメータを実装したトランスポンダチップであり、1つのチップに4つのトランスポンダコアが実装されている。そのため、輻輳状態

¹⁷ Acknowledgement (肯定応答)

¹⁸ ID Error Rate

における通信手法のロバスト性を実証評価することが期待される。

RFID システムは幅広い分野を基盤として成立する技術である。特に識別効率の向上についてはシステムレベルやアルゴリズム、アプリケーションを含む広い視野を持つことも重要であるが、さらに電磁結合やアンテナ、半導体物性や実装技術などに関する深い見識も必要とされる高度な技術である。本研究は通信方式および高位モデルからシステムを具体化するトップダウン・アプローチに基づくシステム設計がこのような高度な技術の実現において重要な意味を持つことを明らかにした。半導体技術の進展に伴う微細化の進歩により SoC¹⁹設計はこれからますます増加していくと考えられる。そのようなチップ設計においては、従来のボトムアップ・アプローチによるハードウェア設計だけでなく、システムレベル設計によるトップダウン・アプローチも重要な位置を占めることが結論づけられた。

¹⁹Systems-on-a-Chip

謝辞

本論文は、筆者が神戸大学大学院自然科学研究科 CS26 において行った研究成果をまとめたものです。ここに御指導、御協力いただいた全ての方に謹んで感謝の意を表します。

本研究の機会を与えていただき、研究のご指導を賜りました神戸大学工学部 情報知能工学科・永田 真 助教授に深く感謝いたします。本研究の遂行にあたっては、研究機材の整備に御尽力いただくとともに、終始にわたって懇切なる御指導、御鞭撻を賜りました。心より感謝いたします。

また、研究室配属当初の指導教員であられました瀧 和男 教授（現 エイ・アイ・エル株式会社代表取締役社長）には、広い見識と鋭い発想で熱心に御指導ならびに御鞭撻、本研究に関して惜しみない御協力、御尽力を戴きました。また、本学退職後も助言や励ましのお言葉をいただきました。心から感謝の意を表します。

本論文をまとめるにあたり貴重な御助言、御指導をいただきました情報知能工学科・吉本 雅彦 教授、電気電子工学科・沼 昌宏 教授、ならびに情報知能工学科・羅 志偉 教授に深く感謝いたします。

研究生生活に関して何かと御世話になり、また研究に限らず様々な視野から日々御議論戴きました情報知能工学科・鎌田 十三郎 助手に深く感謝の意を表します。

同じ研究グループとして、様々な御協力を戴きました CS26 卒業生である大野 修治 氏に御礼申し上げます。本研究の高位モデル構築にあたって、特にエミュレータによるバックエンド設計に関わる諸作業を手伝っていただきました。心より感謝いたします。また、郷地 直樹 氏ならびに近成 聡志 氏には統合シミュレーション環境に関して様々なアイデアを提供戴き、環境の構築における諸作業を手伝って戴きました。深く感謝いたします。

後輩として様々な御協力ならびに無理難題を聞いて戴きました CS26 LSI グループの諸氏に心から感謝申し上げます。特に、研究テーマは異なるものの同じ博士課程において日々の議論を通じて研究に多大なる刺激を与えていただきました森本 薫夫 氏、野口 宏一朗 氏、小坂 大輔 氏、深澤 光弥 氏、松野 哲郎 氏に感謝いたします。

研究室での日常生活においてお世話になりました CS26 の皆様に感謝申

し上げます。特に、無償奉仕であるにも拘らず計算機環境の構築ならびに維持に日々奮闘戴いた CS26 計算機管理者の諸氏にはあらためて感謝の意を表します。

本研究のチップ実装については、東京大学大規模集積システム設計教育研究センター提供による Cadence ツールおよび Synopsys ツールを用いて設計し、同センターを通して株式会社 日立製作所、大日本印刷 株式会社、ローム株式会社、凸版印刷株式会社の各社協力の下で試作が行われたものです。関係各位に深く感謝いたします。

最後に私をここまで育てて下さいました両親、ならびに温かく見守ってくれた祖父母、兄、義姉に心より感謝します。

参考文献

- [1] I. Satoh, “Mobile applications in ubiquitous computing environments,” *IEICE Transactions on Communications*, Vol. E88-B, No. 3, pp. 1026–1033, 2005.
- [2] I. Satoh, “A spatial model for ubiquitous computing services,” *IEICE Transactions on Communications*, Vol. E88-B, No. 3, pp. 923–931, 2005.
- [3] K. Sakamura, “T-engine – the open platform for the ubiquitous computing age,” in *Proceedings of 1st IEEE Asian Solid-State Circuits Conference*, pp. 3–6, 2005.
- [4] R.A. Force, “RAF history,” <http://www.raf.mod.uk/history/>. [4]:
- [5] S.H. Weigart, “Physical security devices for computer subsystems: A survey of attacks and defenses,” in *Proceedings of Workshop on Cryptographic Hardware and Embedded Systems*, Vol. 1965 of Lecture Notes in Computer Science, pp. 302–317, Springer-Verlag, 2000.
- [6] R. Imura, “The world’s smallest RFID μ -chip, bringing about new business and lifestyles,” in *Symposium on VLSI Circuits 2004 Digest of Technical Papers*, pp. 120–123, 2004.
- [7] R. Want, “RFID: A key to automating everything,” *Scientific American*, pp. 56–65, 2004.
- [8] G. Asada, M. Dong, T.S. Lin, F. Newberg, G. Pottie, W.J. Kaiser, and H.O. Marcy, “Wireless integrated network sensors: Low power systems on a chip,” in *Proceedings of 24th IEEE European Solid-State Circuits Conference*, pp. 9–16, 1998.
- [9] N. Cho, S.J. Song, S. Kim, S. Kim, and H.J. Yoo, “A 5.1- μ W UHF RFID tag chip integrated with sensors for wireless environmental



- monitoring,” in *Proceedings of 31st IEEE European Solid-State Circuits Conference*, pp. 279–282, 2005.
- [10] S. Weis, S. Sarma, R. Rivest, and D. Engels, “Security and privacy aspects of low-cost radio frequency identification systems,” in *Proceedings of International Conference on Security in Pervasive Computing – SPC 2003*, Vol. 2802 of Lecture Notes in Computer Science, pp. 454–469, Springer-Verlag, 2003.
- [11] A. Juels and R. Pappu, “Squealing euros: Privacy protection in RFID-enabled banknotes,” in *Proceedings of Financial Cryptography – FC’03*, Vol. 2742 of Lecture Notes in Computer Science, pp. 103–121, Springer-Verlag, 2003.
- [12] International Organization for Standardization, “ISO/IEC 18004: Information technology – automatic identification and data capture techniques – QR code 2005 bar code symbology specification,” 2006.
- [13] S. Masui, W. Yokozeki, M. Oura, T. Ninomiya, K. Mukaida, Y. Takayama, and T. Teramoto, “Design and applications of ferroelectric nonvolatile SRAM and flip-flop with unlimited read/program cycles and stable recall,” in *Proceedings of IEEE Custom Integrated Circuits Conference 2003*, pp. 403–406, 2003.
- [14] H. Nakamoto, D. Yamazaki, T. Yamamoto, H. Kurata, S. Yamada, K. Mukaida, T. Ninomiya, T. Ohkawa, S. Masui, and K. Gotoh, “A passive UHF RFID tag LSI with 36.6% efficiency CMOS-only rectifier and current-mode demodulator in 0.35 μ m FeRAM technology,” in *IEEE International Solid-State Circuits Conference 2006 Digest of Technical Papers*, pp. 310–311 and 655, 2006.
- [15] M. Usami, A. Sato, H. Tanabe, T. Iwamatsu, S. Maegawa, and Y. Ohji, “An SOI-based 7.5 μ m-thick 0.15 $\times$ 0.15mm² RFID chip,” in *IEEE International Solid-State Circuits Conference 2006 Digest of Technical Papers*, pp. 308–309 and 655, 2006.
- [16] S. Masui, E. Ishii, T. Iwasaki, Y. Sugawara, and K. Sawada, “A 13.56MHz CMOS RF identification transponder integrated circuit

- with a dedicated CPU,” in *IEEE International Solid-State Circuits Conference 1999 Digest of Technical Papers*, pp. 162–163, 1999.
- [17] A. Juels, “RFID security and privacy: a research survey,” *IEEE Journal of Selected Areas in Communications*, Vol. 24, No. 2, pp. 381–394, 2006.
- [18] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic approach to “privacy-friendly” tags,” in *Proceedings of RFID Privacy Workshop*, MIT, MA, USA, 2003.
- [19] S. Inoue and H. Yasuura, “RFID privacy using user-controllable uniqueness,” in *Proceedings of RFID Privacy Workshop*, MIT, Massachusetts, USA, 2003.
- [20] A. Juels, R. Rivest, and M. Szydlo, “The blocker tag: Selective blocking of RFID tags for consumer privacy,” V. Atluri, editor, in *Proceedings of Conference on Computer and Communications Security – ACM CCS*, pp. 103–111, Washington, DC, USA, 2003, ACM, ACM Press.
- [21] G.M. Gaukler, “*RFID in supply chain management*,” ProQuest / UMI, 2006.
- [22] S. Sarma, K. Ashton, and D. Brock, “The networked physical world,” White Paper MIT-AUTOID-WH-001, Auto-ID Center, MIT, Cambridge, 2000, available at <http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-001.PDF>.
- [23] R. Glidden, C. Bockorick, S. Cooper, C. Diorio, D. Dressler, V. Gutnik, C. Hagen, D. Hara, T. Hass, T. Humes, J. Hyde, R. Oliver, O. Onen, A. Pesavento, K. Sundstrom, and M. Thomas, “Design of ultra-low-cost UHF RFID tags for supply chain applications,” *IEEE Communications Magazine*, Vol. 42, No. 8, pp. 140–151, 2004.
- [24] S. Briole, C. Pacha, K. Goser, A. Kaiser, R. Thewes, W. Weber, and R. Brederlow, “AC-only RF ID tags for barcode replacement,” in *IEEE International Solid-State Circuits Conference 2004 Digest of Technical Papers*, p. 438, 2004.



[22]:

- [25] M. Böhm, A. Ullmann, D. Zipperer, A. Knobloch, W.H. Glauert, and W. Fix, “Printable electronics for polymer RFID applications,” in *IEEE International Solid-State Circuits Conference 2006 Digest of Technical Papers*, pp. 270–271, 2006.
- [26] E. Cantatore, T. Geuns, A. Gruijthuijsen, G. Gelinck, S. Drews, and D. de Leeuw, “A 13.56MHz RFID system based on organic transponders,” in *IEEE International Solid-State Circuits Conference 2006 Digest of Technical Papers*, pp. 272–273 and 653, 2006.
- [27] P.F. Baude, D.A. Ender, T.W. Kelley, M.A. Haase, D.V. Muyres, and S.D. Theiss, “Organic semiconductor RFID transponders,” in *IEEE International Electron Devices Meeting 2003 Technical Digest*, pp. 8.1.1–8.1.4, 2003.
- [28] S. Tanaka, T. Ishifuji, T. Saito, M. Shida, and K. Nagai, “A coding scheme for field-powered RF IC tag systems,” in *Symposium on VLSI Circuits 1998 Digest of Technical Papers*, pp. 230–231, 1998.
- [29] U. Karthaus and M. Fischer, “Fully integrated passive UHF RFID transponder IC with 16.7- μ W minimum RF input power,” *IEEE Journal of Solid-State Circuits*, Vol. 38, No. 10, pp. 1602–1608, 2003.
- [30] U. Kaiser and W. Steinhagen, “A low-power transponder IC for high-performance identification systems,” *IEEE Journal of Solid-State Circuits*, Vol. 30, No. 3, pp. 306–310, 1995.
- [31] C. Alippi and G. Vanini, “An application-level methodology to guide the design of intelligent-processing, power-aware passive RFIDs,” in *Proceedings of 2005 IEEE International Symposium on Circuits and Systems*, pp. 5509–5512, 2005.
- [32] D. Friedman, H. Heinrich, and D.W. Duan, “A low-power CMOS integrated circuit for field-powered radio frequency identification tags,” in *IEEE International Solid-State Circuits Conference 1997 Digest of Technical Papers*, pp. 294–295, 1997.

- [33] J. Chabloz, C. Müller, F. Pengg, A. Pezous, C. Enz, and M.A. Dubois, “A low-power 2.4GHz CMOS receiver front-end using BAW resonators,” in *IEEE International Solid-State Circuits Conference 2006 Digest of Technical Papers*, pp. 320–321 and 656, 2006.
- [34] M.D. Scott, B.E. Boser, and K.S.J. Pister, “An ultralow-energy ADC for smart dust,” *IEEE Journal of Solid-State Circuits*, Vol. 38, No. 7, pp. 1123–1129, 2003.
- [35] B.A. Warneke and K.S.J. Pister, “An ultra-low energy microcontroller for smart dust wireless sensor networks,” in *IEEE International Solid-State Circuits Conference 2004 Digest of Technical Papers*, pp. 316–317, 2004.
- [36] T. Umeda, H. Yoshida, S. Sekine, Y. Fujita, T. Suzuki, and S. Otaka, “A 950MHz rectifier circuit for sensor networks with 10m-distance,” in *IEEE International Solid-State Circuits Conference 2005 Digest of Technical Papers*, pp. 256–257, 2005.
- [37] S. Jain and S.R. Das, “Collision avoidance in a dense RFID network,” in *Proceedings of 1st International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*, pp. 49–56, 2006.
- [38] D. Kunz, “Channel assignment for cellular radio using neural networks,” *IEEE Transactions on Neural Networks*, Vol. 10, No. 1, pp. 1443–1455, 1999.
- [39] M. Duque-Anton, D. Kunz, and B. Ruber, “Channel assignment for cellular radio using simulated annealing,” *IEEE Transactions on Vehicular Technology*, Vol. 42, pp. 14–21, 1993.
- [40] W.K. Lai and G.G. Coghill, “Channel assignment for a homogenous cellular network with genetic algorithms,” *IEEE Transactions on Vehicular Technology*, Vol. 45, pp. 91–96, 1996.
- [41] D.W. Engels, “The reader collision problem,” White Paper MIT-AUTOID-WH-007, Auto-ID Center, MIT, Cambridge, 2001, available at <http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-007.PDF>.

[41]:



- [42] J. Waldrop, D.W. Engels, and S.E. Sarma, “Colorwave: An anticollision algorithm for the reader collision problem,” in *Proceedings of IEEE 2003 International Conference on Communications*, Vol. 2, pp. 1206–1210, 2003.
- [43] J. Waldrop, D.W. Engels, and S.E. Sarma, “Colorwave: A MAC for RFID reader networks,” in *Proceedings of IEEE 2003 Wireless Communications and Networking Conference*, pp. 1701–1704, 2003.
- [44] J.K. Ho, “Solving the reader collision problem with a hierarchical Q-learning algorithm,” Master’s thesis, Massachusetts Institute of Technology, 2003.
- [45] J. Ho, D. Engels, and S. Sarma, “HiQ: a hierarchical Q-learning algorithm to solve the reader collision problem,” in *Proceedings of 2006 International Symposium on Applications and the Internet Workshops*, pp. 88–91, 2006.
- [46] C.J.C.H. Watkins, “*Learning from Delayed Rewards*,” PhD thesis, Kings College University of Cambridge, 1989.
- [47] A.G. Barto, S.J. Bradtke, and S.P. Singh, “Learning to act using real-time dynamic programming,” *Artificial Intelligence*, pp. 81–138, 1995.
- [48] S.M. Birari and S. Iyer, “PULSE: A MAC protocol for RFID networks,” in *Proceedings of Embedded and Ubiquitous Computing*, Vol. 3823 of Lecture Notes in Computer Science, pp. 1036–1046, Springer Berlin, 2005.
- [49] L.A. Burdet, “RFID multiple access methods,” Seminar “Smart Environments”, ETH Zürich, 2004.
- [50] D.H. Shih, P.L. Sun, D.C. Yen, and S.M. Huang, “Taxonomy and survey of RFID anti-collision protocols,” *Computer Communications*, Vol. 29, No. 11, pp. 2150–2166, 2006.
- [51] K. Finkenzeller, “*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*,” John Wiley & Sons, 2nd ed., 2003.

- [52] S.H. Kim, M.K. Shin, and P. Park, "A new tree-based tag anti-collision protocol for RFID systems," in *Proceedings of 2006 International Conference on Communications in Computing*, pp. 83–86, 2006.
- [53] J.I. Capetanakis, "Tree algorithms for packet broadcast channels," *IEEE Transactions on Information Theory*, Vol. 25, No. 5, pp. 505–515, 1979.
- [54] M.A. Kaplan and E. Gulko, "Analytic properties of multiple-access trees," *IEEE Transactions on Information Theory*, Vol. 31, No. 2, pp. 255–263, 1985.
- [55] J.F. Hayes, "An adaptive technique for local distribution," *IEEE Transactions on Communications*, Vol. 26, No. 8, pp. 1178–1186, 1978.
- [56] B.S. Tsybakov and V.A. Mikhailov, "Free synchronous packet access in a broadcast channel with feedback," *Problemy Peredachi Informatsii*, Vol. 14, No. 4, pp. 32–59, 1978.
- [57] M. Jacomet, A. Ehrcsam, and U. Gehrig, "Contactless identification device with anticollision algorithm," in *Proceedings of IEEE Conference on Circuits, System, Computers and Communications*, pp. 4–8, 1999.
- [58] H.S. Choi, J.R. Cha, and J.H. Kim, "Fast wireless anti-collision algorithm in ubiquitous ID system," in *Proceedings of 2004 IEEE 60th Vehicular Technology Conference*, Vol. 6, pp. 4589–4592, 2004.
- [59] H.S. Choi, J.R. Cha, and J.H. Kim, "Improved bit-by-bit binary tree algorithm in ubiquitous ID system," in *Proceedings of Advances in Multimedia Information Processing - PCM 2004*, Vol. 3332 of Lecture Notes in Computer Science, pp. 696–703, Springer-Verlag, 2004.
- [60] T.P. Wang, "Enhanced binary search with cut-through operation for anti-collision in RFID systems," *IEEE Communication Letters*, Vol. 10, No. 4, pp. 236–238, 2006.

- [61] D.R. Hush and C. Wood, “Analysis of tree algorithms for RFID arbitration,” in *Proceedings of 1998 IEEE International Symposium on Information Theory*, pp. 107–116, 1998.
- [62] C. Law, K. Lee, and K.Y. Siu, “Efficient memory-less protocol for tag identification,” in *Proceedings of 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pp. 75–84, 2000.
- [63] F. Zhou, D. Jing, C. Juang, and H. Min, “Optimizing the power consumption of passive electronic tags for anti-collision schemes,” in *Proceedings of 5th International Conference on ASIC*, pp. 1213–1217, 2003.
- [64] F. Zhou, C. Chen, D. Jing, C. Huang, and H. Min, “Evaluating and optimizing power consumption of anti-collision protocols for applications in RFID systems,” in *Proceedings of 2004 International Symposium on Low Power Electronics and Design*, pp. 357–362, 2004.
- [65] J. Myung and W. Lee, “Adaptive binary splitting: A RFID tag collision arbitration protocol for tag identification,” *The Journal of SPECIAL ISSUES on Mobility of Systems, Users, Data and Computing*, Vol. 11, No. 5, pp. 711–722, 2006.
- [66] J. Myung and W. Lee, “Adaptive binary splitting: A RFID tag collision arbitration protocol for tag identification,” in *Proceedings of 2005 2nd International Conference on Broadband Networks*, Vol. 1, pp. 347–355, 2005.
- [67] J. Myung and W. Lee, “An adaptive memory-less tag anti-collision protocol for RFID networks,” in *Proceedings of IEEE INFOCOM 2005, 24th Annual Joint Conference on IEEE Computer and Communications Societies*, 2005.
- [68] W. Yen, “Hash based collision resolution for passive RFID tags,” in *Proceedings of 2004 International Computer Symposium*, pp. 423–428, 2004.

- [69] M.A. Bonuccelli, F. Lonetti, and F. Martelli, “Randomized hashing for tag identification in RFID networks,” Technical Report 2005-TR-38, Università di Pisa, 2005.
- [70] J.Y. Kim, B.S. Kang, J.W. Jwa, and D.Y. Yang, “Bin-slotted hybrid search algorithm for multiple RFID arbitration,” in *Proceedings of 2006 International Conference on Wireless Networks*, pp. 164–169, 2006.
- [71] W. Szpankowski, “Packet switching in multiple radio channels: Analysis and stability of a random access system,” *Computer Networks*, Vol. 7, pp. 17–26, 1983.
- [72] H. Vogt, “Efficient object identification with passive RFID tags,” in *Proceedings of 1st International Conference on Pervasive Computing*, Vol. 2414 of Lecture Notes in Computer Science, pp. 98–113, Springer-Verlag, 2002.
- [73] B. Zhen, M. Kobayashi, and M. Shimizu, “Framed ALOHA for multiple RFID objects identification,” *IEICE Transactions on Communications*, Vol. E88-B, No. 3, pp. 991–999, 2005.
- [74] International Organization for Standardization, “ISO/IEC 18000-7: Information technology – radio frequency identification for item management – part 7: Parameters for an active RFID interface communications at 433 MHz,” 2004.
- [75] F.C. Schoute, “Control of ALOHA signaling in a mobile radio trunking system,” in *Proceedings of International Conference on Radio Spectrum Conservation Techniques*, pp. 38–42, 1980.
- [76] J.E. Wieselthier, A. Ephremides, and L.A. Michaels, “An exact analysis and performance evaluation of framed ALOHA with capture,” *IEEE Transactions on Communications*, Vol. 37, No. 2, pp. 125–137, 1989.
- [77] F.C. Schoute, “Dynamic frame length ALOHA,” *IEEE Transactions on Communications*, Vol. 31, No. 4, pp. 565–568, 1983.

- [78] H. Vogt, "Multiple object identification with passive RFID tags," in *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, Vol. 3, p. 6, 2002.
- [79] W.T. Chen and G.H. Lin, "An efficient anti-collision method for tag identification in a RFID system," *IEICE Transactions on Communications*, Vol. E89-B, No. 12, pp. 3386–3392, 2006.
- [80] J.R. Cha and J.H. Kim, "Novel anti-collision algorithms for fast object identification in RFID system," in *Proceedings of 2005 11th International Conference on Parallel and Distributed Systems*, Vol. 2, pp. 63–67, 2005.
- [81] Phillips Semiconductors, "I-CODE1 system design guide," Application Note, 2002, available at <http://www.nxp.com/products/identification/icode/ic/index.html>.
- [82] International Organization for Standardization, "ISO/IEC 18000-3: Information technology – radio frequency identification for item management – part 3: Parameters for air interface communications at 13,56 MHz," 2004.
- [83] Magellan Technology, "A comparison of RFID frequencies and protocols," White Paper, 2006, available at <http://www.magtech.com.au/downloads/>.
- [84] International Organization for Standardization, "ISO/IEC 18000-2: Information technology – radio frequency identification for item management – part 2: Parameters for air interface communications at below 135 kHz," 2004.
- [85] International Organization for Standardization, "ISO/IEC 18000-4: Information technology – radio frequency identification for item management – part 4: Parameters for air interface communications at 2,45 GHz," 2004.
- [86] International Organization for Standardization, "ISO/IEC 18000-6: Information technology – radio frequency identification for item

- management – part 6: Parameters for air interface communications at 860 to 960 MHz,” 2004.
- [87] R. Mäusl, “*Digitale Modulationsverfahren*,” Hüthig Verlag, 1985.
- [88] A. Mansukhani, “*Wireless Digital Modulation*,” Applied Microwave & Wireless, 1996.
- [89] C.H. Yang, Y.H. Lin, S.C. Liu, and T.D. Chiueh, “Design of a low-complexity receiver for impulse-radio ultra-wideband communication systems,” in *Proceedings of 2004 IEEE International Symposium on Circuits and Systems*, Vol. 4, pp. 125–128, 2004.
- [90] S. Yoshizumi, T. Terada, J. Furukawa, Y. Sanada, and T. Kuroda, “All digital transmitter scheme and transceiver design for pulse-based ultra-wideband,” in *Proceedings of IEEE Conference on Ultra-Wideband Systems and Technologies*, 2003.
- [91] J.S. Lee and L.E. Miller, “*CDMA Systems Engineering Handbook*,” Mobile Communications Series, Artech House Publishers, 1998.
- [92] C.E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, Vol. 27, pp. 379–423 and 623–656, 1948.
- [93] C. Berrou and A. Glavieux, “Near optimum error correcting coding and decoding: Turbo codes,” *IEEE Transactions on Communications*, Vol. 44, No. 10, pp. 1261–1271, 1996.
- [94] L.R. Bahl, J. Cock, F. Jelinek, and J. Raviv, “Optimal decoding of linear codes minimizing symbol error rate,” *IEEE Transactions on Information Theory*, Vol. 20, No. 3, pp. 284–287, 1974.
- [95] J.L. Walsh, “A closed set of normal orthogonal functions,” *American Journal of Mathematics*, Vol. 45, pp. 5–24, 1923.
- [96] W. Feller, “*An Introduction to Probability Theory and Its Application*,” Vol. 1, John Wiley & Sons Inc., 3rd ed., 1968.
- [97] P. Frey and D. O’Riordan, “Verilog-AMS: Mixed-signal simulation and cross domain connect modules,” in *Proceedings of 2000*

IEEE/ACM International Workshop on Behavior Modeling and Simulation, pp. 103–108, 2000.

- [98] M. Vlach, “Programming interface requirements for an AMS simulator,” in *Proceedings of 2004 IEEE International Symposium on Circuits and Systems*, pp. 640–643, 2004.
- [99] R.W. Chang, “Synthesis of band-limited orthogonal signals for multi-channel data transmission,” *Bell System Technical Journal*, Vol. 45, pp. 1775–1796, 1966.
- [100] K. David and T. Benkner, “*Digitale Mobilfunksysteme*,” B. G. Teubner Stuttgart, 1996.
- [101] R. Gold, “Optimal binary sequences for spread spectrum multiplexing,” *IEEE Transactions on Information Theory*, pp. 619–621, 1967.
- [102] T. Kasami, “*Weight Distribution Formula for some class of cyclic codes*,” Vol. R-285 of AD 632574, pp. 268–274, Coordinated Science Lab, University of Illinois at Urbana-Champaign, 1966.
- [103] S. Glisic and B. Vucetic, “*Spread Spectrum CDMA Systems for Wireless Communications*,” Mobile Communications Series, Artech House Publishers, 1997.
- [104] T. Ojanperä and R. Prasad, editors, “*Wideband CDMA for Third Generation Mobile Communications*,” Mobile Communications Series, Artech House Publishers, 2001.
- [105] IEEE Standards Association, “Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the 2.4 GHz band,” IEEE Standard, 1999, available at <http://standards.ieee.org/getieee802/802.11.html>.
- [106] Bluetooth SIG, “Specification of the Bluetooth system version 2.0 + EDR,” 2004, available at <http://www.bluetooth.com/Bluetooth/Learn/Technology/Specifications/>.

[105]:



[106]:



発表論文一覧

本研究に関する発表論文

学術雑誌

- [1] Y. Fukumizu, S. Ohno, M. Nagata, and K. Taki, “Communication scheme for a highly collision-resistive RFID system,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E89-A, No. 2, pp. 408–415, 2006.
- [2] Y. Fukumizu, M. Nagata, and K. Taki, “Back-end design of a collision-resistive RFID system through high-level modeling approach,” *IEICE Transactions on Electronics*, Vol. E89-C, No. 11, pp. 1581–1590, 2006.
- [3] Y. Fukumizu, N. Gochi, M. Nagata, and K. Taki, “A mixed circuit and system level simulation technique of collision resistant RFID system,” *IEICE Transactions on Electronics*, Vol. E90-C, No. 6, 2007. to appear

国際会議

- [4] Y. Fukumizu, S. Ohno, M. Nagata, and K. Taki, “A highly collision resistive RFID system,” in *Proceedings of 5th Asia-Pacific Symposium on Information and Telecommunication Technologies*, pp. 223–228, 2003.
- [5] Y. Fukumizu, S. Ohno, M. Nagata, and K. Taki, “A design of transponder IC for highly collision resistive RFID systems,” in *Proceedings of IEEE 2004 Asia-Pacific Conference on Advanced System Integrated Circuits*, pp. 438–439, 2004.
- [6] Y. Fukumizu, S. Ohno, M. Nagata, and K. Taki, “Design of RFID front-end circuitry enabling CDMA-based collision resistance,” in

Proceedings of 2004 International Conference on Solid State Devices and Materials, pp. 400–401, 2004.

学術講演

- [7] 福水 洋平, 大野 修治, 永田 真, 瀧 和男, “超多重応答を可能にする RFID システムの LSI 設計と評価,” 情報処理学会 DA シンポジウム 論文集, pp. 73–78, 2003.
- [8] 大野 修治, 福水 洋平, 永田 真, 瀧 和男, “TD-CDMA による輻輳制御を用いた RFID システム向けトランスポンダの IC 設計と評価,” 電子情報通信学会 信学技報 ICD2004-138, pp. 19–24, 2004.
- [9] 福水 洋平, 永田 真, 瀧 和男, “超多重 RFID システムの高位モデル化とバックエンド設計への応用,” 電子情報通信学会 信学技報 ICD2006-114, pp. 29–34, 2006.

口頭発表

- [10] 福水 洋平, 大野 修治, 永田 真, 瀧 和男, “超多重応答を可能にする RFID システムの LSI 設計と評価,” 第 7 回システム LSI ワーク ショップ, 2003.
- [11] 福水 洋平, 大野 修治, 永田 真, 瀧 和男, “超多重 RFID タグ向け変復調回路の検討,” 第 4 回シリコンアナログ RF 研究会, 2005.

図一覧

1.1	各標準規格に基づくバーコードのパターン例	3
1.2	二次元バーコードのパターン例	4
1.3	RFID システムの構成	7
1.4	隣接するリーダによる電磁干渉	10
1.5	複数のリーダによる通信の衝突	12
1.6	Colorwave のスロット構成	13
1.7	環境によるエージェントの強化学習	13
1.8	HiQ アルゴリズムにおけるリーダ群の階層構造	14
1.9	複数のトランスポンダと単一のリーダ間における衝突	16
1.10	Bit-by-bit アルゴリズムの木構造	19
1.11	Bit-by-bit による認識フロー例	20
1.12	Binary search アルゴリズムの木構造	21
1.13	Binary search による認識フロー例	22
1.14	Binary tree アルゴリズムの木構造	23
1.15	Binary tree による認識フロー例	24
1.16	Adaptive binary splitting の認識フロー例	24
1.17	Query tree アルゴリズムの木構造	26
1.18	Query tree の認識フロー例	27
1.19	Hashed query による認識フロー例	28
1.20	Bin-slotted hybrid search による認識フロー例	30
1.21	各種の衝突防止アルゴリズムに対する本研究の位置づけ	34
2.1	超多重 RFID システムの応用例	39
2.2	RFID 向け 13.56 MHz 帯の電界強度	42
2.3	RFID システムの構成図	43
2.4	超多重 RFID システムにおける通信の概要: (a) システム の状態遷移図、(b) 通信システムのシーケンス図	44
2.5	インパルスによる一次変調波形	46
2.6	TS-CDMA 方式による多重化の概念	48
2.7	ランダムスロットシフト方式のシーケンス例	51

2.8	トランスポンダのデータフロー図	55
2.9	トランスポンダのブロック図	56
2.10	位相シフトの抽出による同期制御の概要: (a) 回路図、(b) 動作フロー図	57
2.11	シュミットトリガによる PoR の動作模式図	58
2.12	BJT によるトランスポンダの一次変調器	59
2.13	トランスポンダ側 DBE のブロック図	59
2.14	リーダのブロック図	61
2.15	リーダに内蔵される相関器のブロック図	62
2.16	SPICE による回路記述: (a) SPICE 向け物理相互作用モデル、(b) 受信信号のシミュレーション結果	64
2.17	MATLAB による回路レベル記述: (a) リーダの等価モデル、(b) シミュレーション波形	65
2.18	テスト用トランスポンダのチップ写真	66
2.19	トランスポンダの RF 回路図: (1) 整流器, (2) キャパシタ, (3) 電圧クランプ, (4) PoR, (5) タイミング抽出	67
2.20	トランスポンダ側 AFE のシミュレーション波形	68
2.21	実験環境の写真	69
2.22	トランスポンダとリーダ間の通信の実測結果 (a) DBE の出力、(b) AFE の出力	70
3.1	チャネルノイズの有無による波形劣化: (a) ノイズのない理想的なチャネルでの通信、(b) ノイズのある現実的なチャネルでの通信	73
3.2	エミュレータのブロック図	74
3.3	エミュレータの写真	75
3.4	リーダの逆拡散プロセスのブロック図: (a) 相関器、(b) 逆拡散モジュール	76
3.5	トランスポンダの拡散プロセスのブロック図	77
3.6	疑似ガウスノイズ生成器のブロック図	78
3.7	TDMA チャネルによる IDER への影響	79
3.8	閾値を変化させたときの IDER と SNR の関係	81
3.9	閾値を変化させたときの SNR と誤って伝送された ID 数の関係	82
3.10	シミュレーションシステムのスクリーンショット	83
3.11	シミュレーションシステムの構成図	84

3.12	多重通信シミュレーションの概要: (a) シミュレータの動作フロー図、(b) 通信状況ウィンドウのスクリーンショット	87
3.13	ノイズ環境下における IDER と TDMA チャンネル数の関係	89
3.14	チャンネル容量と IDER の関係	90
3.15	チャンネルの分配率による IDER/NGID への影響	91
3.16	トランスポンダ DBE の設計チップ	93
4.1	ISE の構造図	97
4.2	ISE のデータフロー図	98
4.3	AFE 部信号フローの拡大図	99
4.4	ISE の動作シーケンス図	101
4.5	実装において直面した問題に対するモデルの修正	102
4.6	ISE の援用による設計チップのレイアウト	103
4.7	AFE 部のシミュレーション結果: (a) ISE により取得した波形、(b) ISE の拡大波形とそれに対応するトランジスタレベルの波形	105
4.8	モデルによる IDER の比較	107
4.9	環境ノイズと IDER の関係	109
4.10	信号とノイズの取り扱いにおける差異: (a) ソフトウェア・シミュレータ、(b) ISE	110
4.11	閾値の選定と IDER/NGID の関係	111
A.1	SS 通信の構成図	148

表一覧

2.1	理論的な導出による RFID システムパラメータの比較 . . .	50
3.1	エミュレーションによるシステムパラメータの性能諸表 . .	80
3.2	シミュレーションにより抽出された最適パラメータ	92
3.3	トランスポンダチップの DBE の設計諸元	93
4.1	トランスポンダチップの設計諸元	104
4.2	モデル比較に用いたパラメータセット	107
4.3	認識を 1,000 回繰り返したときのシミュレーション時間の 比較	108
4.4	性能評価に用いたパラメータセット	108

付録 A

通信の多重化

A.1 概要

RFID¹ システムが複数のトランスポンダによる応答を同時に許容するには、何らかの方法で通信内容の衝突を回避しなければならない。そのために適用される衝突防止アルゴリズムとしては様々なものが提案されているが、その全てが多重通信技術に基づいている。多重通信技術はチャネル多重化の実現方法によって

- FDMA²
- TDMA³
- Orthogonal Frequency Division Multiplexing (OFDM)
- Space Division Multiple Access (SDMA)
- CDMA⁴

に分類することができる。

A.2 FDMA

多重通信手法として古くから用いられてきたFDMAは、送信者ごとに異なる周波数帯域を割り当て、情報の授受には割り当てられた周波数の搬送波を用いることによって混信を起らないようにする方法である。

この方法では複雑な制御を必要としないので、比較的簡単に実現できる。一方、送受信双方に周波数可変の発振器を搭載する必要がある。また、混信を避けるために通信チャネル間にガードバンドを設けなければならない。また、同時応答数によっては広大な帯域幅を必要とする。また、同時

¹Radio Frequency Identification

²Frequency Division Multiplex Access

³Time Division Multiple Access

⁴Code Division Multiple Access

にアクセス可能な識別タグ数も割り当てることのできる周波数帯域と識別信号の占有する帯域幅から一意に定まり、限界を超えた同時通信はできない。

テレビやラジオなどの放送システムだけでなく、初期のアナログ携帯電話やコードレスフォンなど広く用いられてきたが、周波数資源の枯渇が唱えられている近年ではデジタルによる通信方式が定着するとともに、徐々に他の方法に置き換えられつつある。

A.3 TDMA

TDMA は同じ周波数の搬送波を複数の送信者で時間分割して使用方法である。一定の時間枠を多数のタイムスロットと呼ばれる非常に短い時間単位に分割する。各送信者は周波数帯域こそ同じであるが、通信を行うスロットがそれぞれ異なっているため、混信することなく通信ができる。

この方法は音声などの連続量を送受信するためには、一定周期間にサンプリングした情報を短い時間枠に収まるように圧縮しなければならず、アナログ通信での適用は困難であった。しかし、通信チャネルのデジタル化により実現が容易になったため、今日では第 2 世代のデジタル携帯電話や Personal Handyphone System (PHS)、Asynchronous Transmission Mode (ATM) など非常に多くの応用がなされている。

TDMA では、送受信のためにシステム全体が完全に同期しなければならない。そのため、同期のための信号を別途、授受する必要がある。時間枠内のスロット数が固定とすれば、FDMA と同様に同時アクセスできる送信者数はスロット数で一意に定まる。

A.4 OFDM

この方法は互いに直交性をもつ多数の搬送波を用意し、それぞれ別の送信者が情報をのせた上でそれらを重ね合わせ得られる多重化であり [99]、一種の FDMA であるとも言える。

異なる周波数の搬送波にて変調ならびに復調するために、搬送波の数だけ発振器が必要とされたので、実装には非常に緻密な同期制御と膨大な回路規模が必要であった。そのため、従来この技術による多重化は実現が困難であった。しかるに、離散フーリエ変換を使うことによって比

較的容易に実現可能となったため、近年は特にデジタル放送や移動体通信の分野で非常に注目されている。

一方、離散フーリエ変換器による OFDM の復調は依然として他の多重化技術と較べて回路規模が大きい。よって、特に小面積かつ超低消費電力が要求される応用には不向きである。

A.5 SDMA

空間をいくつかに分割し、それぞれに異なる通信チャンネルを割り当てることによって通信多重を行う方法として SDMA がある [100]。

これは、微弱な電波反応を指向性を持つアンテナで受信することにより達成される。個々の送信者の電力を著しく弱め、かつ送信時に指向性を持たせる。受信側はこれをアダプティブアレイのような指向性のアンテナを用いて受信する。指向性のために他の送信者による電波が干渉せず、したがって多重通信が実現される。

RFID においてはマラソン大会など競技大会における走者の順位決定などに用いられるが、リーダに大がかりで複雑なアンテナ装置が必要であるため導入コストを抑えることが難しい。そのため、この方式は非常に限られた応用にのみ用いられる。

A.6 CDMA

現在、次世代の移動体通信システムの中核技術として最も用いられている多重化通信方式である。CDMA は Spread Spectrum (SS) に基づいて実現される。ここで、SS 通信の模式図を Figure A.1 に示す。

CDMA は送信者ごとにそれぞれ異なる符号を割り当て、送信者はその符号を用いて信号スペクトルを拡散する。その拡散した信号は一次変調を経て、全ての送信者で共有する通信チャンネルに送出される。受信側では全ての拡散信号が合成された形で得られるが、この信号に送信者と同じ拡散符号の相関を取ることによって情報が復元される [91]。拡散したスペクトルを復元するには、拡散に用いた符号が不可欠であるため、秘匿性にも優れているといった特徴を持つ。そのため、古くから軍用通信に供されてきたが、今では民間でも広く利用されている。

CDMA に用いられるスペクトルの拡散方法として、主に Frequency Hopping-CDMA (FH-CDMA) と DS-CDMA の 2 種類が利用されている。

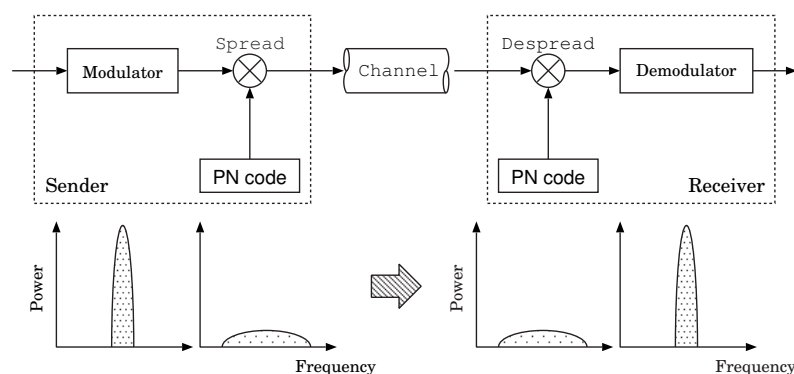


Figure A.1: SS 通信の構成図

FH 方式は搬送波の周波数をホッピングパターンという特定の順序にしたがって順次変化させて拡散を行う方法であり、そのため超高速なシンセサイザを必要とし、特に小面積を要求される移動体通信には不向きである。ホッピングパターンがわからなければ信号の復元が不可能なため、情報の秘匿性に優れている。

一方、DS 方式は情報源よりも高速に変化する拡散符号を直接、掛け合わせるによって拡散を行う方式である。拡散符号はランダム性を持つ疑似ノイズが用いられることが多く、この符号を知らなければ情報が復元できないので、FH 方式と同じく秘匿性に優れている。拡散符号間の干渉を防ぐために、自己相関ならびに相互相関が非常に低い符号を選定する必要がある。このため、拡散符号としては一般的に直交符号である Walsh 符号 [95]、あるいは疑似ランダム符号である Gold 符号 [101] や Kasami 符号 [102] が用いられる。

この CDMA では他の多重化方式と異なり、同時アクセス数が想定値よりも多少超過しても分離可能であるという特色がある [103]。また、DS 方式により多重アクセスを実現すると副搬送波を生成する必要がないが、送信側の拡散処理と受信側の逆拡散処理を同期して行わなければならないので、システムの複雑度は FDMA や TDMA よりも高い。秘匿性やノイズに対するロバスト性が高いだけでなく帯域を効率よく利用できることから、近年では特に注目されており第 3 世代携帯電話 [104] だけでなく無線 LAN [105] や Bluetooth [106] など様々な応用がなされている。

略語一覧

ABS	Adaptive Binary Splitting
ACK	Acknowledgement (肯定応答)
AFE	Analog Front-end
AMS	Analog/Mixed-Signal (アナログ／ミックスシグナル)
ASK	Amplitude Shift Keying (振幅変調)
ATM	Asynchronous Transmission Mode
BHS	Bin-slotted Hybrid Search
BJT	Bi-polar Junction Transistor (バイポーラ接合トランジスタ)
BP³	Bi-phase Pulse Position
BS	Binary search
BT	Binary Tree
CDMA	Code Division Multiple Access
CMOS	Complementary MOS
CRC	Cyclic Redundancy Check (巡回冗長検査)
CSMA	Carrier Sense Multiple Access
DBE	Digital Back-end
DCS	Distributed Color Selection
DFF	Data Flip-flop
DLL	Dynamic Linkage Library (動的リンクライブラリ)
DS-CDMA	Direct Sequence-CDMA
EEPROM	Electrically Erasable and Programmable ROM
FDMA	Frequency Division Multiple Access
FH-CDMA	Frequency Hopping-CDMA

FIFO	First-in-first-out (先入れ先出し)
FPGA	Field-Programmable Gate Array
FSK	Frequency Shift Keying (周波数変調)
FeRAM	Ferroelectric RAM (強誘電体メモリ)
GUI	Graphical User-Interface
HPF	High-Pass Filter (高域通過フィルタ)
HQ	Hashed query
HiQ	Hierarchical Q-learning
IC	Integrated Circuit (集積回路)
IDER	ID Error Rate (ID 誤り率)
IMS	Inventory Management System
ISE	Integrated Simulation Environment (統合マルチレベル・シミュレーション環境)
LDPC	Low Dencity Parity Checking (低密度パリティ検査)
LED	Light-Emission Diode (発光ダイオード)
LFSR	Linear Feedback Shift Register (線形帰還シフトレジスタ)
LNA	Low-noise Amplifier (低ノイズ増幅器)
LRC	Longitudinal Redundancy Check (水平冗長検査)
MIT	Massachusetts Institute of University (マサチューセッツ工科大)
MOSFET	Metal Oxide Semiconductor Field Effect Transistors (金属酸化膜半導体電解効果トランジスタ)
MRAM	Magnetoresistive RAM (磁気抵抗メモリ)

NGID	Number of Ghost IDs (ゴースト ID 数)
NVRAM	Non-Volatile RAM (不揮発メモリ)
OCR	Optical Character Recognition (光学文字認識)
OFDM	Orthogonal Frequency Division Multiplexing
OOP	Object-Oriented Programming (オブジェクト指向プログラミング)
PHS	Personal Handyphone System
PLI	Program Language Interface (プログラム言語インタフェース)
POS	Point-of-Sale
PRSG	Pseudo Random Sequence Generator (疑似乱数系列生成回路)
PSK	Phase Shift Keying (位相変調)
PoR	Power-on Reset
QT	Query Tree
QT-im	Query Tree incremental matching
QT-sl	Query Tree short long
RFID	Radio-Frequency Identification
RS	Reed Solomon
SCM	Supply-Chain Management
SDMA	Space Division Multiple Access
SNR	Signal-to-Noise Ratio (信号対ノイズ比)
SRFF	Set-Reset Flip-flop
SS	Spread Spectrum
SoC	Systems-on-a-Chip
TDMA	Time Division Multiple Access
TEG	Test Element Group
TS-CDMA	Time Slotting-Code Division Multiple Access
UWB-IR	Ultra Wideband-Impulse Radio
VDCS	Variable DCS

XOR	eXclusive OR (排他的論理和)
s-ALOHA	Slotted ALOHA



