# ゲートアレイ混載P2ROM™の開発

関野　芳正　　福山　弘幸

データやプログラムを格納するデバイスとして，不揮発性メモリは，さまざまな用途で使用されている。不揮発性である特徴から，システム立上げ時のブートプログラムや，電子辞書やメモリカード等のデータ格納が代表的な用途である。

近年，ユーザシステムの高性能化に伴い，独自のインタフェース機能や特殊な追加機能を搭載したカスタム仕様が要求されるようになってきた。システムを高性能化するために適した仕様や重要視する性能が，ユーザごとに異なるためである。

今回，カスタム仕様を容易に実現するため，ゲートアレイを混載したP2ROM™*1) を開発した。ゲートアレイを混載することで，カスタム仕様となる部分の設計をASIC（Application Specific Integrated Circuit）設計と同等とすることができる。ゲートアレイ混載チップを開発し，その応用例として，近年特に注目されている個人情報保護に適したメモリカード用ROMとして，強固なセキュリティ機能の搭載を検討したので報告する。

## P2ROM™とは

P2ROM™とは，アセンブリプロセスまで終了したデバイスに，テストプロセスでユーザデータを書き込み出荷することをビジネスモデルとした当社独自の商品である。

一般的に，不揮発性メモリはフラッシュメモリに代表される書き換え可能なメモリと，マスクROMに代表される書き換え不可能なメモリの2つに分類される。書き換え可能なメモリは，データを記録する用途に使われることが多く，デジタルカメラや携帯音楽機器等の一時的な記録媒体を得意分野としている。書き換え不可能なメモリは，書き込み済みデータを提供する用途に使われることが多く，電子辞書や書き換え不要なメモリカード等の記録媒体を得意分野としている。P2ROM™は，書き換え不可能なメモリに属し，電子辞書やメモリカード等で使用されているが，そのビジネスモデルで差別化を実現している。

データ提供を目的とした不揮発性メモリの場合，データの書き込み方式によって差別化することができる。マスクROMはウェハプロセスでデータの書き込みを実施しているため，ユーザから提供されたデータをもとにマスクを作成し，ウェハプロセスとアセンブリプロセス，テストプロセスを経てようやく出荷される。したがってデータ入手から出荷まで，数週間から1ヶ月前後の時間を必要とし，マスク作成の費用も発生する。

それに対し，P2ROM™では，データ入手から最短2日で出荷することも可能である。これは，P2ROM™が1回だけ電気的な書き込みが可能なデバイスである特徴を活用することで実現している。ユーザから提供されたデータは，最終工程であるテストプロセスで電気的な書き込みを実施しているため，データ入手から出荷までの期間を短くすることが可能となる。

短納期での出荷は，ユーザでの在庫数量を最小限にできるメリットがある。また，ユーザが開発中の場合は，データ修正に対し迅速に対応できるメリットがある。実機での評価時にデータ修正が必要となった場合，数日で修正版を入手して確認作業を継続できるため，効率的な検証が可能となる。これは，実際にP2ROM™を必要とする実機での評価直前まで，デバック作業が行えるというメリットでもある。

## ゲートアレイ混載の必要性

大規模化，複雑化するカスタム仕様を短い開発期間で実現するためには，ASIC設計手法の導入が不可欠となる。ユーザでASIC設計した機能も取り込めるようになり，高付加価値化を実現できる。

新規デバイスを開発する場合，開発期間の短縮が重要な設計課題となる。カスタム仕様では，特定ユーザ向けとなるため，ユーザが必要としている納期を達成できなければ商品価値がなくなる場合もある。そのため，納期達成が大前提となり，開発期間の短縮が重要となる。

P2ROM™をはじめとするメモリLSIの場合，インバータ回路やアンド回路等の論理回路だけではなく，トランジスタレベルで設計した回路やアナログ回路を多用している。

*1) P2ROMは沖電気工業(株)の商標です。

そのため，回路設計，パターン設計共，人手による作業となり，カスタム仕様の設計も人手による作業で対応している。

従来のカスタム仕様は，既存機能の部分改良やインタフェース仕様に簡単な機能を追加する程度の改良であり，簡単な変更であったため，人手による設計でも開発期間への影響は少なかった。ところが，近年ではコマンド方式インタフェースの導入や，読み出したデータの加工等の複雑な機能要求が増えてきている。そのため，人手による設計では膨大な作業が必要となり，開発期間の増加が問題となってきた。

大規模化，複雑化するカスタム仕様を短期間に設計するため，ゲートアレイを混載しASIC設計手法を取り入れることを決めた。機能によって異なるが，ASIC設計手法を取り入れた場合の開発期間の見積りは，人手による設計に比べ約1/3以下となった。

また，人手による設計ではできなかったが，ユーザでASIC設計された機能の取り込みも可能となった。

## ゲートアレイ混載チップとその応用

**図1**に今回開発したゲートアレイ混載チップのチップイメージ図を示す。ゲートアレイ部は，P2ROM™メモリセルコア部と入出力回路部の間に配置した。

今回試作したチップは，ゲートアレイ部のロジック回路がチップ全体の制御を行う方式とした。外部から入力した信号は，入出力回路部を介してゲートアレイ部に入力する。ゲートアレイ部では，入力した信号に従いメモリセルコア部制御信号とデータ出力制御信号を生成している。メモリセルコア部は，制御信号に従ってデータの読み出し動作を行い，読み出されたデータは，ゲートアレイ部を介して入出力回路部に伝達される。入出力回路部では，データ出力制御信号に従いデータを出力する。

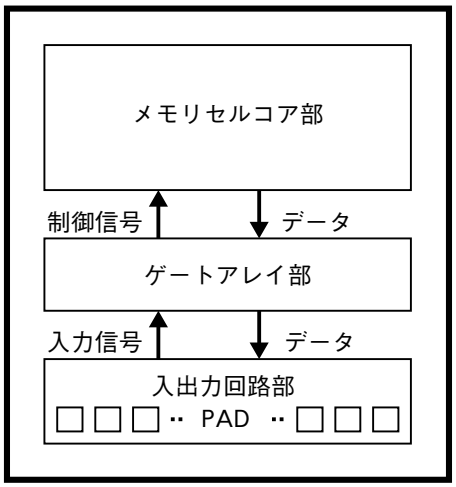


図1　チップイメージ

コマンド方式のインタフェースや読み出したデータの加工機能の使用例として，近年注目が集まっているセキュリティ機能が挙げられる。高度なセキュリティ機能のためには複雑な暗号技術が必要となり開発期間の増大が問題となる。しかし，ASIC設計手法を用いれば短期間で開発できるため，ゲートアレイ混載チップの応用デバイスとして有効性が期待できる。

## 暗号技術

情報に関するセキュリティ問題は，次の3つにまとめることができる。1つ目は，不正な手段で他人のデータを参照する盗聴，または盗視の問題，2つ目は，他人のデータの内容を書き換える改ざんの問題，そして3つ目は，他人が当事者のように振る舞う，なりすましの問題である。暗号技術は，これらセキュリティ問題の対策として非常に重要な技術である。

**図2**に暗号方式の概念図を示す。暗号化の方式には，共

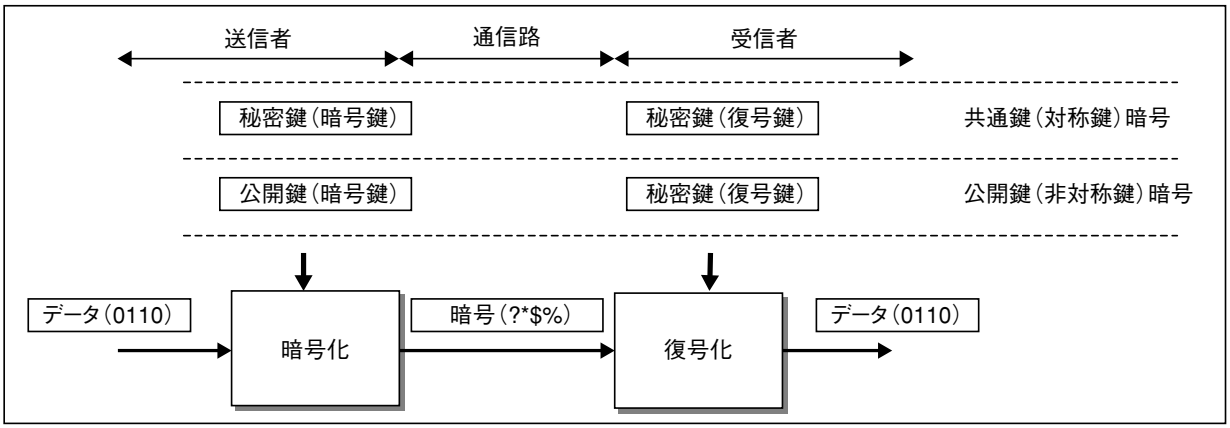


図2　暗号方式

通鍵暗号方式と公開鍵暗号方式がある。共通鍵暗号方式とは，情報の暗号化，復号化に単一の鍵（共通鍵）を用いる。この方式は非常にシンプルであるため，高速化や小型化が可能である。一方，公開鍵暗号方式とは，情報の暗号化，復号化に2つの鍵を用いる。この片方の鍵を公開鍵といい，もう一つの鍵を秘密鍵という。公開鍵によって暗号化されたデータは，秘密鍵によってのみ復号化できるので，公開鍵を公開しても問題がない。

## メモリデータの暗号化

冒頭で述べたとおり，不揮発性メモリであるP2ROM™は，電子辞書やメモリカード等で利用される情報の記録媒体として使われることが多い。これらの用途において，記録される情報は，機器メーカの側でP2ROM™に書き込まれ，そして機器ユーザに提供される。このとき，機器メーカは，データの複製等ユーザによる不正な使用を防止する必要があるが，特に，個人情報が記録されている場合には，そのデータの漏洩を防止する必要がある。そのため，これらデータの記録媒体として使われるP2ROM™には，セキュリティ機能の搭載が強く求められている。

P2ROM™にデータ暗号機能を搭載することで，P2ROM™に格納されたデータのセキュリティを保証することが可能となる。P2ROM™のデータ暗号化とは，具体的には，P2ROM™が持つ2つの通信路の一方，もしくは双方を暗号化する。暗号化する通信路の1つはコマンド入力経路であり，もうひとつはデータ出力経路である。

P2ROM™と混載したゲートアレイ部に暗号機能を搭載した場合のブロック図を**図3**に示す。

コマンド入力経路を暗号化する場合，P2ROM™は暗号データの受信者となる。そのため，暗号化されたコマンド入力を，復号鍵を使って復号化する機能を持つ。P2ROM™制御回路は，復号化された命令に従い，たとえばリードコマンド等のシーケンスをP2ROM™へ入力する。また，データ出力経路を暗号化する場合，P2ROM™は暗号データの送信者となるため，暗号鍵を使ってデータを暗号化する機能を持つことになる。

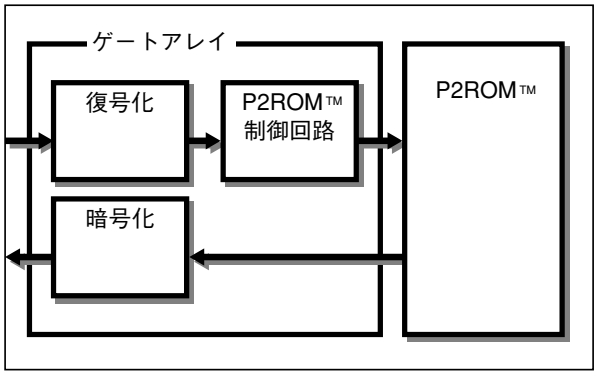


図3　ゲートアレイ混載P2ROM™ブロック図

暗号化，復号化で使われる鍵は，不揮発性メモリに格納される。この暗号鍵，もしくは復号鍵を知ることの困難さ，ならびに改ざんすることの困難さが，暗号の強さを測る重要なファクターとなる。FLASH-ROMのように書き換えが可能な不揮発性メモリでは，鍵の格納場所を解析され，鍵が改ざんされる危険性を持っている。これに対しP2ROM™は，そのデータを書き換えできないという特徴から，鍵が改ざんされる心配がなく，FLASH-ROMに比べ強固な暗号を実現できる。

次に，暗号化に要する処理時間を考える。P2ROM™のデータ出力経路を強固に暗号化できれば，P2ROM™に格納されたデータのセキュリティを保証することができる。ただし，データ出力経路上での暗号処理時間は，データの読み出し時間に直接影響を及ぼすため，この経路に強固な暗号アルゴリズムを適用するとP2ROM™の性能は低下する。こうしたことから，出力データの暗号化に，入力コマンドの暗号化を組み合わせることが効果的な使い方となる。すなわち，出力データ経路に比べアクセス頻度の少ない入力コマンド経路の暗号を強固にすることで，出力データ経路の暗号化をシンプルで高速なものにでき，かつP2ROM™として強固な暗号化が実現できる。

## 暗号機能を持つP2ROM™のテスト方法

ゲートアレイ部に暗号機能を搭載することで，P2ROM™に格納されたデータのセキュリティを保証するわけであるが，チップの出荷検査には特別な考慮が必要となる。

**図4**にテストパターンとP2ROM™の構成図を示す。暗号機能を搭載したP2ROM™を出荷検査するためには，暗号化されたコマンドを入力する必要があり，そして，暗号化された出力データを復号化する必要がある。

## ゲートアレイ混載P2ROM™の設計

商品ごとにさまざまな機能をゲートアレイ領域で実現するため，ゲートアレイ領域に搭載する回路を短TATで設計できる環境を用意している。ゲートアレイ回路の論理設計には，論理合成，論理Sim，スタティックタイミング解析，スキャン挿入等ASIC設計と同等の設計フローを用いることが可能である。さらに，ゲートアレイ領域のレイアウト設計においては，自動配置，自動配線が可能である。また，ゲートアレイ領域のチップ内配置位置，

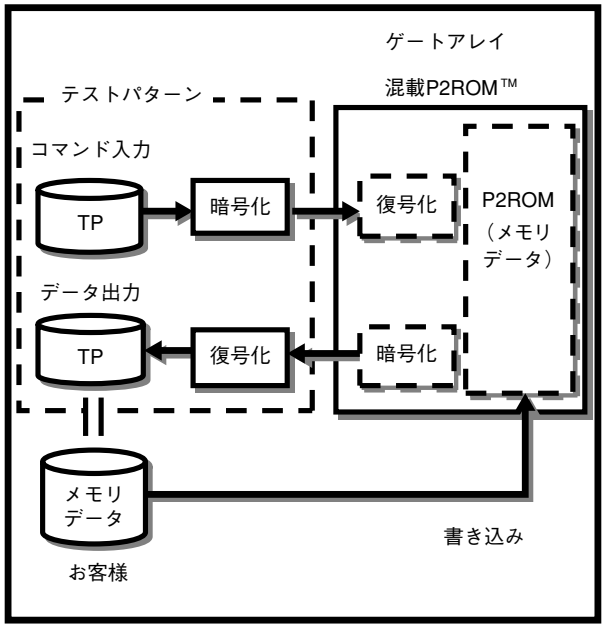


図4　テストパターン構成図

領域サイズ，そして領域境界にある端子位置はあらかじめ決められている。このことにより，ゲートアレイ領域のレイアウトデータを混載チップにはめ込むだけで，既にレイアウトが完了しているP2ROM™領域と接続される。

ゲートアレイ領域には，暗号回路とその他ロジック回路がランダムロジックとして配置される。また，自動配線であることから，一般的にその配線レイアウトは多層でかつ複雑化されている。これらのことは，暗号に対する耐タンパー性を向上させる。

以上のように，P2ROM™にゲートアレイを混載することは，ロジック回路の設計容易性を向上させることに加え，暗号強度の向上を実現する。

## 試　作　結　果

ゲートアレイ混載128Mビット P2ROM™を試作し，正常動作を確認した。ASIC設計手法の検証を目的としたため，ゲートアレイ部には，外部クロック信号同期型の読み出し回路を設計し搭載した。電源電圧範囲Vcc＝3.0V～3.6V，周囲温度範囲Ta＝0℃～80℃で測定し，アクセス速度23ns，動作時消費電流18mAを確認した。ただし，これらの値は制御方式によって影響されるため参考値である。

## ま　と　め

現在，64Mビット品と128Mビット品の開発を終了し，ファミリー品展開として，256Mビット品の開発を着手した。将来的にはさらに大容量品への展開を計画している。

ゲートアレイを活用すればインタフェース機能のカスタマイズだけではなく，さまざまな機能を実現できる。複雑な機能を搭載するためには大きなゲート規模が必要となり，それは，アプリケーションによっても異なる。今回は，過去に人手設計した機能の実現を目標とし20Kゲート規模とした。将来的には，品種展開としてゲート規模を増やすことも視野に入れ，一般的に使用されているさまざまなセキュリティ方式の搭載を可能とするため40Kゲート規模の搭載を検討している。 ◆◆

## ●筆者紹介

関野芳正：Yoshimasa Sekino. シリコンソリューションカンパニー デザイン本部 P2ROM設計部
福山弘幸：Hiroyuki Fukuyama. シリコンソリューションカンパニー デザイン本部 IP設計部