

## Stratix III のデザイン・セキュリティ

### はじめに

重要なシステム・ファンクションに対する FPGA の使用が増加するにつれて、FPGA 内に実装されたデザインおよび IP (Intellectual Property) の保護がますます重要になっています。アルテラの Stratix® III デバイスは、高度暗号化規格 (AES) を不揮発性および揮発性キーのプログラミングと併用して、デザインを複製、リバース・エンジニアリング、および改ざんから保護する初めての高集積、高性能 FPGA です。Stratix III のデザイン・セキュリティ・ソリューションの安全性を高め、AES キーを保護するために、多数のセキュリティ機能が実装されてきました。このソリューションは、デザイン段階で社外のセキュリティ・コンサルタントによって精査され、彼らからのフィードバックに基づいて改善が行われました。このホワイト・ペーパーでは、Stratix III のデザイン・セキュリティ・ソリューションで提供されるセキュリティ保護について、詳細に説明しています。

### SRAM ベース FPGA デザイン・セキュリティ

SRAM ベース FPGA は揮発性で、コンフィギュレーション・ファイルを保存するための外部メモリを必要とするため、複製、リバース・エンジニアリング、および改ざんという 3 つのセキュリティ・リスクが生じます。

#### 複製

FPGA の複製とは、デザインの動作を理解せずにそれとまったく同じコピーを作成することをいいます。デバイスは、メモリ・デバイスからデザインを読み出すか、電源投入時にコンフィギュレーション・ファイルがメモリ・デバイスから FPGA に送られる際に、それをキャプチャすることによって複製できます。盗用されたデザインは、他の FPGA をコンフィギュレーションするのに使用できます。この方法が知的財産盗用の主な形態であり、設計者に重大な収益の損失をもたらす恐れがあります。

#### リバース・エンジニアリング

リバース・エンジニアリングとは、コンフィギュレーション・ファイルを解析して、レジスタ・トランスファ・レベル (RTL) または回路図形式で、オリジナル・デザインを再作成することをいいます。再作成されたデザインを改造して、競争力を高めることができます。この形態の知的財産盗用は複製よりも複雑で、通常は深い技術的専門知識が必要です。また、多大な時間とリソースも必要であり、場合によっては、デザインを初めから作成するよりも多くの作業が必要になることもあります。

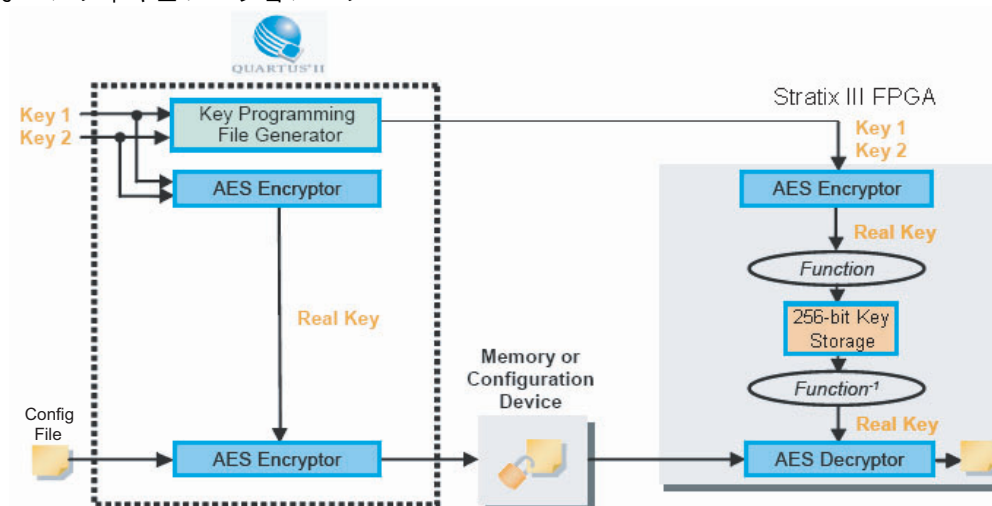
#### 改ざん

デバイスに格納されたデザインを変更したり、それを別のデザインに置き換えることは改ざんとみなされます。改ざんされたデバイスには、システムを誤動作させたり、機密データを盗用する機能を持つ有害なデザイン・コードが含まれている可能性があります。この種のデザイン・セキュリティの侵害は、軍用、財務用、およびゲーム用アプリケーションにおける特有の問題です。今日、改ざんは、不正なサービスやプレミアム・サービスにアクセスするためにデザインが変更される可能性があるコンシューマ市場でも問題になりつつあります。

### Stratix III デザイン・セキュリティ・ソリューション

Stratix III デバイスは SRAM ベースの FPGA です。Stratix III FPGA はデザイン・セキュリティを提供するために、コンフィギュレーション・ビットストリーム暗号化に 256 ビットのセキュリティ・キーを使用します。図 1 に示す安全なコンフィギュレーション・フローは、Quartus II ソフトウェアでの合成、フィッティング、およびタイミング解析後に実現されます。したがって、ハードウェアの設計者は、Mentor Graphics 社の Precision Synthesis ソフトウェアでデザインを最適化し、Mentor Graphics 社の ModelSim® シミュレーション・ソフトウェアでデザインがセキュリティ・キーを適用可能なことを検証した後で、安全なコンフィギュレーション機能を適用することができます。

図 1. 安全なコンフィギュレーション・フロー




以下の3つのステップで、安全なコンフィギュレーションを行うことができます。

1. セキュリティ・キーを Stratix III FPGA 内にプログラム : Quartus® II ソフトウェアには、キー・プログラミング・ファイルを作成するために、256 ビット・ユーザ定義キー（キー 1 およびキー 2）が必要です。次に、キー 1 およびキー 2 の情報が収められたキー・プログラミング・ファイルが、JTAG インタフェースを介して Stratix III FPGA 内にロードされます。Stratix III の内蔵 AES 暗号化エンジンは、キー 2 をキー 1 で暗号化することにより、リアル・キー（ステップ 3 でのコンフィギュレーション・データの復号化に使用）を生成します。このリアル・キーは独自のファンクションによって処理されてから、256 ビットのキー・ストレージに格納されます。このストレージは揮発性（SRAM ベース）または不揮発性（ポリ・ヒューズ・ベース）のいずれも使用できます。
2. コンフィギュレーション・ファイルを暗号化して外部メモリ内に格納 : Quartus II ソフトウェアは、コンフィギュレーション・ファイルを暗号化するために、ステップ 1 で使用したのと同じ 256 ビット・ユーザ定義キー（キー 1 およびキー 2）を要求します。Quartus II の AES 暗号化エンジンは、キー 2 をキー 1 で暗号化することによってリアル・キーを生成します。リアル・キーはコンフィギュレーション・ファイルの暗号化に使用されます。暗号化されたコンフィギュレーション・ファイルは、コンフィギュレーション・デバイスやフラッシュ・デバイスなどの外部メモリ内にロードされます。
3. Stratix III FPGA のコンフィギュレーション : システムのパワーアップ時に、外部メモリ・デバイスから暗号化されたコンフィギュレーション・ファイルが Stratix III FPGA に送られます。次に、Stratix III FPGA 内の 256 ビット・キーが独自ファンクションの逆動作によって処理され、リアル・キーが生成されます。Stratix III の内蔵 AES 復号化エンジンが、このリアル・キーを使用してコンフィギュレーション・ファイルを復号化し、自身をコンフィギュレーションします。

## Stratix III のキー・プログラミング・ソリューション

アルテラは、JTAG インタフェースを介したデザイン・セキュリティ・キー・プログラミング用の各種ソリューションを提供し、オンボードおよびオフボードでのキー・プログラミングをサポートします。

 揮発性キーおよび不揮発性キーをプログラムするためのステップは、「Stratix III デバイス・ハンドブック Volume 1」の「Stratix III デバイスのデザイン・セキュリティ」に記載されています。詳細はアルテラまたは販売代理店にご確認ください。

## AES 暗号化アルゴリズム

AES は Federal Information Processing Standard (FIPS-197) で、機密情報の保護を目的として使用するために合衆国政府機関が承認しています。この標準規格は、商業的にまた世界的に広く採用されるものと見込まれています。

AES は、データの暗号化と復号化を 128 ビットのブロック単位で行う共通ブロック暗号です。暗号化されたデータに対して、バイト置換、データ・ミキシング、データ・シフティング、およびキー追加を含む一連の変換が行われます。

AESには、128ビット、192ビット、256ビットの3つの異なるキー・サイズがあります。Stratix III FPGAでは、セキュリティと効率の両方が得られるように、256ビットのAESキー・サイズが使用されています。NIST (National Institute of Standards and Technology) によると、データ暗号化標準 (DES) キーを数秒で解読できるマシンを構築できたとしても、そのマシンで256ビットのAESキーを解読するのに、149兆年以上かかることが研究によって判明しているとのことです。Stratix IIIのAES実装は、FIPS-197標準規格に準拠していることが確認されています。

## AES 復号化ブロック

復号化ブロックの主な機能は、以下のとおりです。

- コンフィギュレーション・データを復号化する必要があるか否かを判断する。
- セキュリティ・モードを決定する。
- データ・ストリームを復号化し、必要に応じてデータを復元する。あるいは、デバイスをコンフィギュレーションする。

暗号化されたデータを受信する前に、256ビットのセキュリティ・キーをデバイス内に入力および格納しなければなりません。不揮発性セキュリティ・キーと、バッテリー・バックアップ付き揮発性セキュリティ・キーのいずれかを選択することができます。不揮発性キーとポリ・ヒューズ・キー検証ビット (ポリ・ヒューズ・キーが存在することを示します) がワнтаイム・プログラマブルのポリ・ヒューズに格納されるのに対し、256ビットの揮発性キーと揮発性キー検証ビット (揮発性キーが存在することを示します) は、外部バッテリー電源でバックアップされる揮発性キー・レジスタに格納されます。

## キー・ストレージ

セキュリティ・キーは、Stratix III FPGA 内のポリ・ヒューズおよび揮発性キー・レジスタに格納されます。ポリ・ヒューズは、不揮発性のワнтаイム・プログラマブル・デバイスです。揮発性キー・ストレージは、デバイスがパワー・ダウンされたときにキーの格納を可能にする外部バックアップ・バッテリーを必要とします。セキュリティ・キーは、通常の製造フロー中に、オンボード (揮発性キーおよび不揮発性キーの両方) またはオフボード (不揮発性キーのみ) の Stratix III FPGA にプログラムすることができます。

## Stratix III FPGA が提供するセキュリティ保護

Stratix III FPGA のデザインは、コンフィギュレーション・ビットストリーム暗号化により、複製、リバース・エンジニアリング、および改ざんから保護されています。

## 複製に対するセキュリティ

Stratix III FPGA のセキュリティ・キーは、いかなるインタフェースを介しても読み出すことができません。セキュリティ・キーが格納されたポリ・ヒューズと揮発性キー・レジスタは、他の数百のポリ・ヒューズに混じってメタル層の下に隠されています。簡単な目視検査で、特定のヒューズまたはレジスタの機能を確認することは非常に困難です。キー・ビットは、スクランブルされて FPGA 内の他のロジックに分散されます。さらに、他のファンクションに使用されるキー・ストレージのプログラミング状態は、デバイスによって異なる可能性があります。このランダム性によって、セキュリティ・キーが格納されているヒューズまたはレジスタを識別するのが一層困難になります。また、たとえキー・ストレージが識別されたとしても、復号化に使用されるリアル・キーは、ストレージ前に独自のファンクションによって処理されるので解明されません。リアル・キーがわからないと、デザインを復号化することはできません。

Stratix III FPGA は、コンフィギュレーション・ファイルのリードバックをサポートしていないので、リードバック・アタックに対して安全です。これにより、FPGA 内でコンフィギュレーション・ファイルが復号化された後で、それをリードバックしようとする試みは阻止されます。

Stratix III のデザインは、セキュリティ・キーを別の FPGA にプログラムし、それを暗号化されたコンフィギュレーション・ファイルでコンフィギュレーションしても複製できません。セキュリティ・キーを Stratix III FPGA にプログラムするには、2つの256ビット・キーが必要です。リアル・キーの生成にAESが使用されているので、セキュリティ・キーからキー1とキー2を生成することは実質的に不可能です。既知の弱いAESキーはありません。

## リバース・エンジニアリングに対するセキュリティ

コンフィギュレーション・ファイルからの Stratix III デザインのリバース・エンジニアリングは、暗号化が行われていない場合でも、非常に困難で時間のかかる作業です。Stratix III のコンフィギュレーション・ファイルには、数百万ビットが収められており、コンフィギュレーション・ファイル・フォーマットは独自かつ機密のものです。Stratix III

デザインのリバース・エンジニアリングを行うには、FPGA または Quartus II デザイン・ソフトウェアのリバース・エンジニアリングによって、コンフィギュレーション・ファイルからデバイス・リソースへのマッピングを解明する必要があります。

Stratix III FPGA 自体のリバース・エンジニアリングも非常に困難です。Stratix III FPGA は、TSMC 社で最先端 65 nm プロセス・テクノロジーに基づいて製造されています。ASIC とは異なり、これらの最先端 FPGA をリバース・エンジニアリングするための標準ツールや知識は容易に得られません。Stratix III FPGA の 1 つのロジック・ブロックをリバース・エンジニアリングし、FPGA 内のキーの場所を発見するだけでも、かなりの時間とリソースを必要とします。

コンフィギュレーション・ビットストリーム暗号化によって、リバース・エンジニアリングはさらに困難になります。セキュリティ・キーを見つけてコンフィギュレーション・ファイルを復号化するのは、それを複製することと同じくらい困難です。セキュリティで保護された Stratix III デザインのリバース・エンジニアリングを行うよりも、競争力のあるデザインを初めから構築する方が簡単で早いかもしれません。

## 改ざんに対するセキュリティ

不揮発性キーはワンタイム・プログラマブルです。改ざん保護ビットが一度セットされると、FPGA は同じキーで暗号化されたコンフィギュレーション・ファイルしか受け入れません。さらに、それ以降のキー・プログラミングは許可しません。暗号化されていないコンフィギュレーション・ファイルや間違っただけの暗号化されたコンフィギュレーション・ファイルで Stratix III FPGA をコンフィギュレーションしようとしても、コンフィギュレーションは失敗します。コンフィギュレーションの失敗は、それが外部メモリ内、外部メモリと FPGA との間の伝送の際、あるいは遠隔通信システムのアップグレード時のいずれかで発生しても、デザインの改ざんの可能性を示唆します。

## サポートされているコンフィギュレーション手法

デザイン・セキュリティ機能は、外部ホスト (MAX<sup>®</sup> II デバイスやマイクロプロセッサ) でファースト・パッシブ・パラレル (FPP) コンフィギュレーション・モードを使用して、Stratix III FPGA をコンフィギュレーションするとき、あるいはアクティブ・シリアル (AS) またはパッシブ・シリアル (PS) コンフィギュレーション手法を使用するとき使用できます。FPP をエンハンスド・コンフィギュレーション・デバイスまたは JTAG ベースのコンフィギュレーションと一緒に使用して Stratix III FPGA をコンフィギュレーションする場合、デザイン・セキュリティ機能は使用できません。ただし、Stratix III デバイスを暗号化する際に選択したセキュリティ・モードによっては、デバイスが選択されたコンフィギュレーション手法しかサポートしない場合があります。



Stratix III デバイスでサポートされているセキュリティ・モード、および各セキュリティ・モードに対応するコンフィギュレーション手法について詳しくは、「Stratix III デバイス・ハンドブック」の「Stratix III デバイスのデザイン・セキュリティ」の章 ([www.altera.co.jp/literature/hb/stx3/stx3\\_siii51014.pdf](http://www.altera.co.jp/literature/hb/stx3/stx3_siii51014.pdf)) を参照してください。

## まとめ

Stratix III FPGA は、設計者の知的財産を保護し、改ざんを防止することにより、これらのデバイスを安全な商用アプリケーションや一般的な軍用アプリケーションに適したものにする、多数のセキュリティ機能を備えた堅牢なデザイン・セキュリティ・ソリューションを提供します。これらのセキュリティ機能によって、設計者は Mentor Graphics 社およびアルテラのデザイン・ツールと検証ツールを使用して設計された製品を安全かつ迅速にお客様に納入でき、技術革新を試験するためのリスクのない手段を提供して、製品を他の競合製品から差別化します。

## 文献

- Federal Information Processing Standards (FIPS-197):  
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- Advanced Encryption Standard Algorithm Validation List:  
<http://csrc.nist.gov/cryptval/aes/aesval.html>



101 Innovation Drive  
San Jose, CA 95134  
(408) 544-7000  
<http://www.altera.com>

Copyright © 2006 Altera Corporation. All rights reserved. Altera, The Programmable Solutions Company, the stylized Altera logo, specific device designations, and all other words and logos that are identified as trademarks and/or service marks are, unless noted otherwise, the trademarks and service marks of Altera Corporation in the U.S. and other countries. All other product or service names are the property of their respective holders. Altera products are protected under numerous U.S. and foreign patents and pending applications, maskwork rights, and copyrights. Altera warrants performance of its semiconductor products to current specifications in accordance with Altera's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Altera assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Altera Corporation. Altera customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.

この資料は英語版を翻訳したもので、内容に相違が生じる場合には原文を優先します。こちらの日本語版は参考用としてご利用ください。設計の際には、最新の英語版で内容をご確認ください。