WP266 (v1.0) 2007 年 7 月 24 日

Spartan-3 ジェネレーション FPGA を使用したセキュリティ ソリューション

著者 : Maureen Smerdon

今日の国際社会で、セキュリティは大きな関心事です。航空機への搭乗、家庭の戸締り、または、新製品の回路設計開始時においても、セキュリティは重大な問題です。家庭では盗難から守るため、適切なセキュリティ対策を備え付けます。電子産業においても、セキュリティは急速に不可欠な存在になってきています。電子設計分野でセキュリティが最先端の問題に発展した理由を理解することは重要です。その理由の 1 つとして、盗難の結果、偽造商品が急増していることが挙げられます。Anti-counterfeiting Coalition (模倣対策連合) の報告によると、これらの偽造商品は経済を脅かし、消費者市場に世界規模の多大な影響を与えています。このホワイト ペーパーでは、デザインのセキュリティに対する最大の脅威を特定し、ザイリンクスの新しい、低コストの Spartan™-3A、Spartan-3AN、および Spartan-3A DSP FPGA の高度なセキュリティ オプションについて述べ、ユーザーの製品および利益をどのように守るかについて説明します。

偽造がもたらす経済的な影響

偽造は、多大かつ回復不可能な損失を収益にもたらすだけでなく、会社の信用を傷つけ、偽造品が市場に出回ることでカスタマ サポートの負担を増加させ、承認および処理が必要な RMA (返品保証) により利益高に影響を及ぼす可能性があります。製品の盗難にあった会社は、評判とイメージ維持のため、偽造またはその可能性がある製品を探し出す必要があります。その会社の将来的な販売および業務の継続も危機にさらされます。

2003 年には、米国での偽造製品取引の推定額は 2870 億ドルで、これは全世界の年間推定額 (4560 億ドル) の 63% に相当します。2004 年、世界関税機構では、偽造品取引が全世界の貿易取引の 5 ～ 7 % を占めると推測しました。この脅威は年間 12 ～ 15% で増加し続け、結果として模造品によって利益に損失が生じています。家電製品、半導体デバイス、バッテリ、自動車部品、通貨、製薬、およびスポーツ製品を含む、すべての産業が影響を受けています。このホワイト ペーパーでは、低コストの FPGA を使用する際に直面する、セキュリティ関連の脅威のうちで重大な 3 つから製品を保護するためにザイリンクスが提供する方法を説明します。

最も頻繁に行われるセキュリティ侵害手法

現在、最も頻繁に使用されるセキュリティ侵害手法は、リバース エンジニアリング、オーバービルディング、およびクローニングです。

リバース エンジニアリングでは、窃取したデザインから競合製品を再現または再構築し、これらを市場で販売します。この場合、デザインをより短時間で構築できるため、研究開発 (R & D) コストを最小化できることが特徴となります。これは、電子産業界の創成期から最も一般的な侵害手法です。

今日、企業が製造を外部に委託するにつれ、新たなセキュリティ侵害、オーバービルディングおよびクローニングの被害を被りやすくなっています。これらについて次に説明します。

オーバービルディングは、外部に製造委託するビジネス モデルで潜在的な懸念事項となっています。この場合、製品が不正に規定量より多く製造され、元の機器製造業者の許可なく、ほかの経路から販売されます。こうして製造された製品が市場で販売される際に、非常に多大な悪影響があることは明らかです。通常、「オーバービルト」 された製品は低コストで販売され、製品の市場への投入も非常に早くなります。

クローニングは、同じまたは異なるラベル表示で、デザイン、IP、または製品の複製を製造することです。この場合、研究開発コストが発生せず、クローンした製品の市場への投入までの期間が大幅に削減されます。

十分なセキュリティとは

設計者はどのように対応すれば良いのでしょうか。まず、突破されないセキュリティはないと認識することが重要です。結局のところ、システムへの侵入は完全には阻止できません。侵入者はデータやデザインが欲しければ、いかなる手段を用いてでもそれを入手します。これは単なるハッカーではなく、十分な資金のある政府または競合企業の場合があります。これを心に留めて、突破されないソリューションを作り出すのではなく、クローニング、オーバービルディング、およびリバース エンジニアリングに共通する脅威から十分に保護する方法を準備する必要があります。

セキュリティについて考察する際、製品の要件に適切なものは何か考える必要があります。たとえば 10,000 ドルのコストがかかるシステムがあることを考えると、製品のコストが 10 ドルである場合、この価格帯のシステムに適切なレベルのセキュリティがあります。これは、FPGA ユーザー自身が評価する必要があります。評価終了後、それに基づいて、どの製品に対して、どのセキュリティ レベルをインプリメントするかを決定できます。ザイリンクスでは、単純な問題から複雑な問題までを解決する、さまざまなソリューションを提供しています。このホワイト ペーパーでは、Spartan-3 ジェネレーション FPGA 内でのセキュリティのインプリメンテーションで、より基本的と考えられるソリューションについて説明します。

さらに高度な手法の使用を考慮される場合は、Spartan-3A および Spartan-3AN FPGA を使用した高度なセキュリティ手法に関する資料をご参照ください。ザイリンクスでは、Spartan 製品以外でも、高度なソリューションを Virtex™ FPGA で提供しています。

Spartan FPGA が柔軟かつ低コストのセキュリティを実現

Spartan-3AN FPGA のオンチップ Flash メモリおよび隠されたビットストリーム

Spartan-3AN デバイスは、コンフィギュレーション データの保存に使用できるオンチップの Flash メモリを提供しています。Flash を外部に接続しないデザインでは、I/O ピンから Flash を読み出しできません。

Spartan-3AN デバイスでは、Flash が FPGA 内にあるため、そのビットストリームがコンフィギュレーション中は隠されています。このコンフィギュレーションでは、デザインが Flash から直接コピー不可であり、デザインのセキュリティの第一歩となります。

コンフィギュレーション セキュリティ

Spartan-3 デバイスに未知のコンフィギュレーション データをダウンロードする事態から保護する最も単純な方法は、モード ピンをハードワイヤ接続し、Flash の自動コンフィギュレーションのみを許可してデータ ピンを切断することです。また、回路への接続がすべてパッケージ内にある場合、BGA または CS パッケージからのピンへの直接接続は非常に困難です。ピンがハードワイヤ接続されている際に異なるコンフィギュレーション データをロードするには、直接 PCB を攻撃する必要があります。

ビットストリーム ジェネレータのセキュリティ レベル

デザインのテストおよびデバッグ段階で、デザイン製品化後のメンテナンスまたは任意の点検のために ICAP (内部コンフィギュレーション アクセス ポート) または ChipScope™ Pro Analyzer コアをデザインに残すように決定できます。ChipScope Pro Analyzer などのソフトウェア機能の一部には、内部ロジックのステータスの読み出しにこれらのマクロが必要です。これは設計者にとっては便利ですが、セキュリティ ホールになる可能性があります。

Bitstream Generator は、NCD ファイルと呼ばれる物理的なインプリメンテーション ファイルの内容に基づいて、コンフィギュレーション ファイル (**.bit**) を作成します。BIT ファイルは、プログラム済み FPGA の動作を定義します。Bitstream Generator には多数のオプションがあり、これらの 1 つにセキュリティ レベル設定があります。Bitstream Generator には、4 つのセキュリティ レベルがあります。最初のレベルはデフォルトで、その他 3 つはオプションであり、追加のセキュリティを提供します。次の表に示すように、リードバック動作は完全に無効にするか、限られたアクセス オプション以外を無効にできます。表 1 に、セキュリティ レベルの設定と機能を示します。

表 1: Bitstream Generator のセキュリティ レベル設定

セキュリティ レベル	説明
なし	デフォルト。すべてのコンフィギュレーションおよびリードバック機能へのアクセスが無制限
レベル 1	SelectMAP または JTAG ポート (外部ピン) の両方からのリードバック機能がすべて無効。ICAP を介したリードバックは有効
レベル 2	全ポートでのリードバック動作がすべて無効
レベル 3	すべてのコンフィギュレーションおよび JTAG ポートからのコンフィギュレーションとリードバック機能がすべて無効。(リードバックとコンフィギュレーションに関しては) レベル 3 で発行および実行できる唯一のコマンドは REBOOT。このコマンドは、デバイスのコンフィギュレーションを消去する。コマンドがデバイス内から実行されることを除いて、これはデバイスで PROG_B ピンを有効にすることと機能的に同一

Bitstream Generator の全オプションの詳細については、UG332 :『Spartan-3 ジェネレーション コンフィギュレーション ユーザーガイド』を参照してください。

Device DNA によるセキュリティ

ザイリンクスでは、Spartan-3A/3AN/3A DSP プラットフォームで Device DNA セキュリティを提供しており、デザイン、IP および組み込まれたコアなどを保護します。Device DNA は各 Spartan-3A/3AN/3A DSP FPGA に固有の 57 ビットの ID です。この ID は特定の FPGA にデザインを関連付ける際に使用できます。FPGA に保存される、設計者が独自に作成したアルゴリズムは、固有の Device DNA の取得方法と、結果の作成方法を定義する数式です。ID は設計者のアルゴリズムを使用して組み合わされ、外部メモリや内部 Flash (Spartan-3AN FPGA デバイスのみ) など、設計者が選択する任意の場所に結果が保存されます。アルゴリズムは設計者のみが知っているため、セキュリティとしては隠されています。

Device DNA の動作

各ファミリでのセキュリティの動作について説明する前に、ソリューションの核について理解しておく必要があります。ザイリンクス FPGA、特に Spartan-3A/3AN/3A DSP FPGA に固有の Device DNA は、デザイン セキュリティのために使用されます。このセクションでは、Device DNA の動作について説明し、特許取得済みの新しい手法で将来のデザインを保護する方法について述べます。

Device DNA とは

Device DNA は、製造プロセス中、Spartan-3A/3AN/3A DSP FPGA にザイリンクスで入力される固有の 57 ビットの識別子です。各 FPGA には固有の ID があり、特定の FPGA に対してデザインの関連付けが可能です。このセキュリティまたはライセンス付けプロセスは完全に柔軟に設計されています。セキュリティまたはライセンス付けプロセスはモデルごとに容易に変更できるため、デザインのセキュリティが向上します。読み出し専用の Device DNA は、外部 JTAG ポートまたは内部 DNA ポートを介してアクセスでき、セキュリティ アルゴリズムへの接続が容易です。

クローニングまたはオーバービルドされたビットストリームのコピーがほかの FPGA に配置された場合、新しい FPGA の Device DNA は違うものになります。Device DNA をチェックするアルゴリズムを使用後、デザインは未認証またはエラーを示す結果を返すため、ユーザーまたは設計者がセキュリティ侵害に対する対応を決定できます。

Device DNA セキュリティの基本

Device DNA セキュリティ プロセスは ATM での取引に類似しています。ATM から現金を引き出す場合、ATM カードを挿入し、タッチ パネルで暗証番号を入力します。カードと暗証番号が銀行に保存されている ID と一致すると、取引は承認されて現金を引き出すことができます。不一致の場合は、取引が拒否されて現金を引き出すことができません。図 1 にセキュリティのフローを示します。

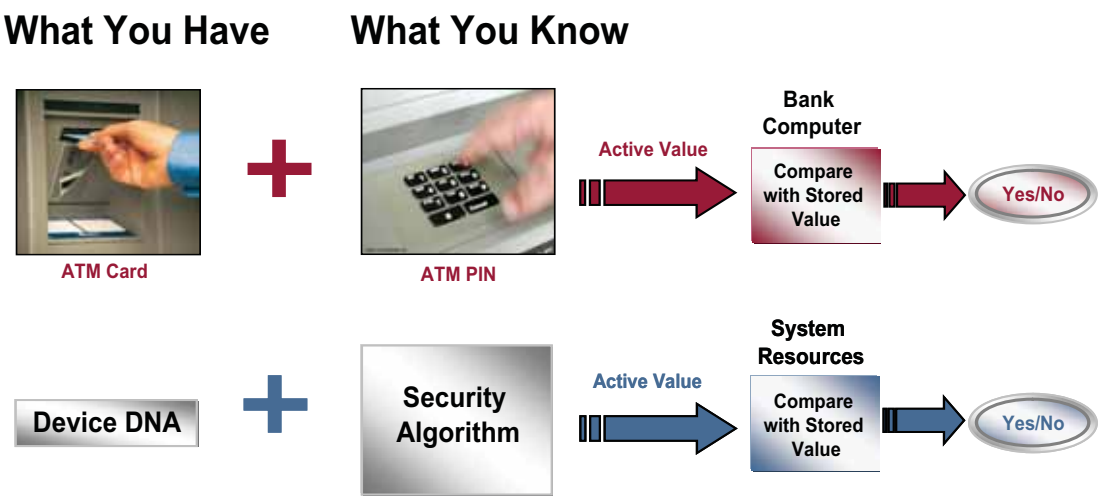

図 1 : セキュリティ フロー

Spartan-3A/3AN/3A DSP デバイスにはセキュリティ アルゴリズムおよび Device DNA の両方が含まれています。Device DNA を使用して、セキュリティ アルゴリズムはチェック値を生成します。Device DNA はデフォルトでは 57 ビットですが、セキュリティ向上のためにビット数を追加可能です。また、Spartan-3AN では、工場で設定された 64 バイトの Flash ID が使用可能で、セキュリティ向上のためにこの ID をアルゴリズムに用いることができます。チェック値は、システム リソースの任意の場所に保存可能です (たとえば、コンフィギュレーション メモリ、ペリフェラル メモリ、システム メモリなど)。Spartan-3AN FPGA の場合は、ワンタイム プログラマブルな 64 バイトのセキュリティ レジスタのユーザー設定フィールドにチェック値を保存できます。このレジスタによって、外部インターフェイスまたはストレージを使用することなく、セキュリティ システム全体が内蔵可能です。

無許可の動作

通常動作中、デバイスに電力が投入されると、FPGA のコンフィギュレーションのためにビットストリームがロードされます。セキュリティ アルゴリズムが Device DNA を読み出し、アクティブ値を生成します。その後、アクティブ値と最初の設定で保存されたチェック値が比較されます。チェック値がアクティブ値と同じ場合は、通常動作が開始できます。2 つの値が不一致の場合、次 のうち 1 つの対応方法を選択して製品を設計可能です。

- 機能停止

  デザインは、完全に機能を停止します。これは、トライステート、ゲートを介したクロック、フリップフロップ クロック イネーブルなどのグローバル制御信号を使用して Spartan FPGA に容易にインプリメント可能です。

- 機能の制限

  デザインの機能が部分的または基本的な動作に制限され、重要な機能を無効またはバイパスさせます。この場合、サードパーティのテスト機関や委託製造業者は製造およびテスト可能であるのと同時に、オーバービルディングが防止できます。システムは、評価モードまたはデモ モードで動作します。

- 時限装置

  デザインでは、あらかじめ設定した時間まですべての機能が動作します。この場合、サードパーティのテスト機関や製造委託業者による製造およびテストが可能になります。システムは、デモ モードまたは IP の評価用に動作します。

- 自己消去 (Spartan-3AN デバイスのみ)

  Flash のセクタ消去および封鎖による保護機能を使用してすべてのセクタを消去し、恒久的に Flash メモリをすべて 0 に固定します。これによって不正なアクセスの繰り返しが防止されます。

Device DNA を使用して Spartan-3A FPGA にセキュリティをインプリメント

これから説明する手法は、デザインのセキュリティ設定に考えられる方法の 1 つです。考えられると述べたのは、これは、家庭に使用するセキュリティ システムを決定するのと似ているからです。世界に錠と鍵が たった 1 つしかない場合は、セキュリティは存在できません。最初の 1 回のみ可能な設定プロセス中に、Spartan-3A/3AN/3A DSP FPGA の Device DNA は、JTAG ポートを介して、または FPGA のファブリック内から読み出しできます。このコード (チェック値) は、コンフィギュレーション メモリやシステム メモリなどのシステムの任意の部分に保存されます。図 2 に、ここで説明する考慮可能なインプリメンテーションを示し、この保存場所を紫色で示します。

Device DNA は青色で示し、「秘密の」セキュリティ アルゴリズムおよびキー / シード コード (これをデザインで使用する場合) を緑色で示します。その後にコンパレータおよび認証された場合と認証されない場合のオプションがあります。

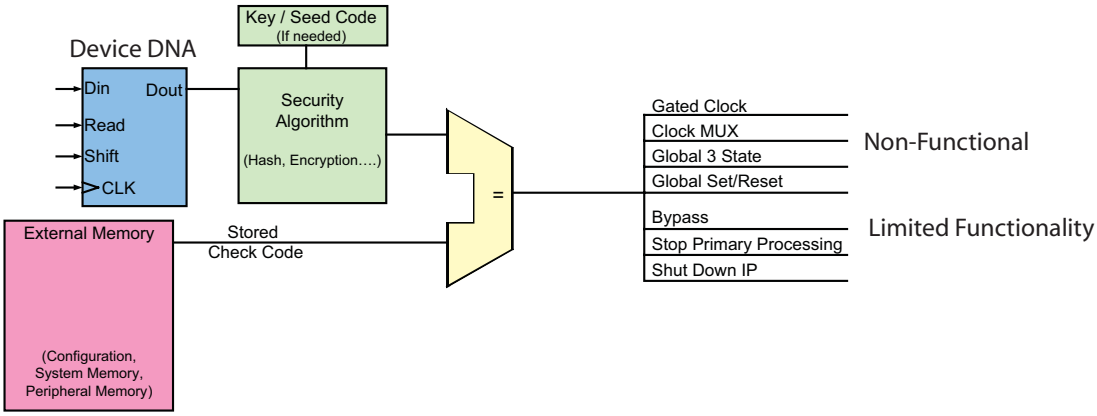

図 2 : Device DNA のセキュリティ例

この設定を使用する場合は、次の手順が実行されます。

1. デバイスに電源が投入され、ビットストリームがコンフィギュレーションのためロードされます。セキュリティ アルゴリズムおよび Device DNA の両方が Spartan-3A デバイスに含まれます。
2. デバイス DNA が読み出され、セキュリティ アルゴリズムに送信されます。
3. セキュリティ アルゴリズムはアクティブ コード (結果) を生成します。
4. アクティブ コードおよび保存されたチェック コードの比較が完了します。
5. 保存されたチェック コードが算出されたアクティブ コードと同じ場合は、デザインは認証されます。
6. 2 つのコードが不一致の場合は、デザインは認証されず、設定に従ってデザインがその後の処理を実行します。認証されないデザインに対して、機能停止、機能制限、時限装置などの処理を複数設定可能です。

繰り返しになりますが、これは考慮可能な単純な手法です。より複雑なセキュリティも同様に容易に設定できます。

Spartan-3AN Device DNA および工場設定の Flash ID によるセキュリティ

不揮発性の FPGA である Spartan-3AN プラットフォームでは、このプロセスは Spartan-3A デバイスとほぼ類似しており、いくつかの向上点が追加されています。第一のセキュリティの向上点は、ビットストリームが FPGA 内部に隠されていることです。これにより、モニタがより困難になります。

第二のセキュリティの向上点は、Spartan-3AN には、固有のシリアル番号が 2 つ (Device DNA および工場設定の Flash ID) Flash メモリにあることです。2 つの固有な ID は、70 バイト以上のシリアル番号で構成され、より大きな数のアルゴリズムが実現可能で、結果としてセキュリティ アルゴリズムの侵害に要する時間が大幅に増加します。デザインはこれによって特定の FPGA および Flash ID の両方に関連付けられます。

2 つの固有な ID を持つことは、現金の引き出しに 2 つの ATM カードが必要な場合に例えられます。現金を引き出す場合は、両方のカードが必要です。カードを 1 枚紛失してしまうと、現金を引き出すことはできませんが、お金は安全です。

第三の向上点は、チェック コードの保存です。Spartan-3AN プラットフォームには、オンチップのセキュリティ レジスタ内にある 64 バイトでワンタイム プログラマブルの特別なユーザー定義フィールドにセキュリティ コードを保存できます。これによって、外部インターフェイスまたはストレージが不要な内蔵型の完全なセキュリティ システムが実現されます。この機能は、全体のセキュリティを向上し、製品のリバース エンジニアリングを一層困難にします。

セキュリティ アルゴリズムはユーザーによって定義可能であり、適正なシステム コストでの適切なセキュリティ レベルのインプリメントが可能になります。セキュリティ アルゴリズムは、セキュリティ システムから基本的に隠されています。セキュリティの侵害防止のため、セキュリティ プロセスの一部が隠されている必要があります。アルゴリズムが未知の値であるため、デザイン レベル セキュリティの要となります。アルゴリズムは FPGA のファブリックにインプリメントされるため、FPGA 内にある大量なコンフィギュレーション ビットのほんの一部となります。ビットの構成や、アルゴリズムの作用を知らない場合は、部外者やクローニングを試みる者には単なる大量な数字の羅列に見えます。図 3 に、Spartan-3AN デバイスを使用したフローの一例の概要を示します。

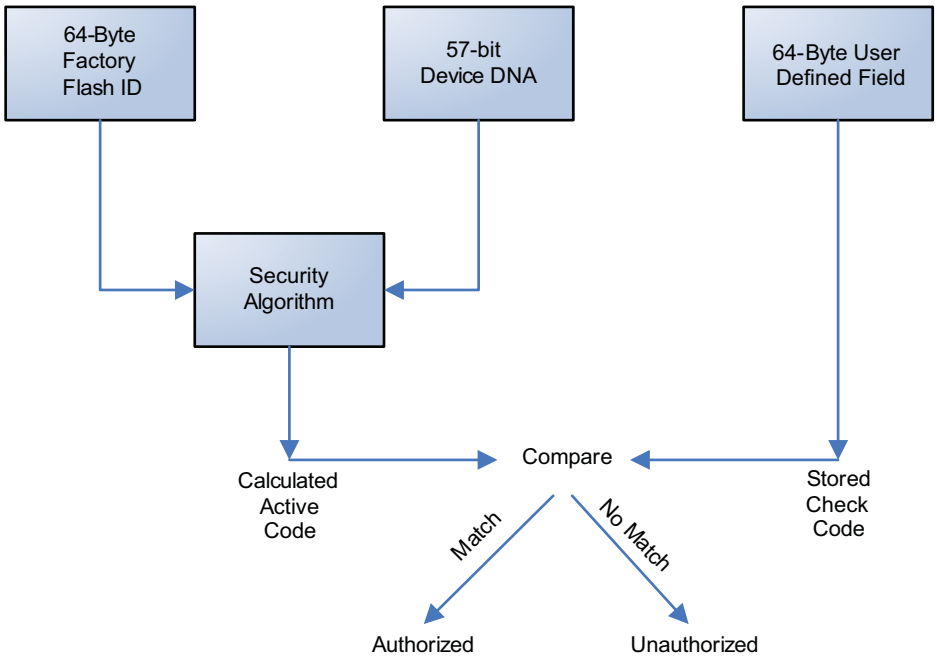

図 3 : Spartan-3AN のセキュリティ

図 4 に示す Spartan-3AN のデザイン レベルのセキュリティは完全内蔵型のセキュリティ ソリューションです。Flash には、FPGA コンフィギュレーション ビットストリームおよびあらかじめ生成されたチェック コードの両方が含まれています。このコードは、信頼の置ける、安全な製造業者または登録プロセスによってワンタイム プログラマブルな Flash ユーザー フィールドに保存されます。

電源投入時には、FPGA は通常通りコンフィギュレーションを実行します。コンフィギュレーション後、FPGA アプリケーションは、関連付けられた Spartan-3AN FPGA でデザインが動作することを確認する回路を含んでいます。Device DNA および工場設定の Flash ID は、セキュリティ アルゴリズムによって読み出されます。ここではアクティブコードが作成され、Flash のユーザー定義フィールドに保存されているチェック コードとこのコードを比

較します。両方のコードが一致する場合、デバイスは認証されます。そうでなければデバイスは不正と判断され、認証されません。

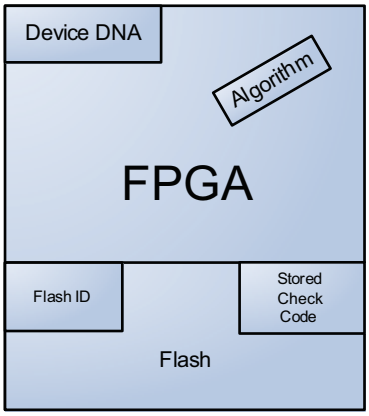

図 4 : Spartan-3AN のセキュリティ

認証がエラーとなった場合の対応が存在することは、Device DNA デザイン レベル セキュリティ手法の利点の 1 つです。ほかの利点として、デザインに完全に統合可能なことが挙げられます。Spartan-3A プラットフォームと同様、認証がエラーとなったデザインへの対応方法は複数あります。

Spartan-3AN プラットフォームのデザイン レベルのセキュリティは、オーバービルディング、クローニングおよびリバース エンジニアリングへの対策を多数提供しています。本書以外にも、低コストの FPGA デザインの保護に関する資料があります。ザイリンクスが提供する、これら 3 つのファミリに関するデザイン保護についての詳細は、『Spartan-3 ジェネレーション コンフィギュレーション ユーザー ガイド』
(**http://japan.xilinx.com/bvdocs/userguides/ug332.pdf**) を参照してください。さらに高度なセキュリティ手法については、**ホワイト ペーパー 267** を参照してください。

ザイリンクスが提供するほかのセキュリティ ソリューション

Virtex-4 および Virtex-5 FPGA では、セキュリティに AES 暗号を使用しています。両ファミリでは、長寿命のバッテリで有効に保たれている揮発性メモリにキー ビットを保存しています。FIPS 140 規格では、電力が切断された場合に「キーを空にする」手法が求められているのは興味深いことです。電源が切断されると、デバイスは暗号化されたビットストリームによって使用不可能となります。

Virtex-5 ファミリは 256 ビットの AES 暗号化 / 暗号解読テクノロジで、非常に高レベルなデザイン セキュリティを達成しています。1.1 X 10^{77} 通りのキーの組み合わせが可能で、ビットストリームは厳重に保護され、正しい暗号解読キーの知識がなければ、クローニングされることはほぼありません。

CoolRunner™-II CPLD は不揮発性で、デザインの保護に便利な機能をいくつか提供しています。CoolRunner-II CPLD にはもともと、複数のビット読み出し / 書き込み保護および不揮発性の EPROM テクノロジといった有益なセキュリティがあります。ビットストリームが直接露出していることはなく、ビットストリームが内部にある場合は、読み出し保護でアクセスを阻止します。また、ユーザーからの情報で、適当な「上位互換可能な」手法で、更にセキュリティを向上できることがわかりました。CoolRunner-II CPLD へのステップ 1 シリコンの導入で、新しいセキュリティ機能 (読み出し保護、バウンダリ スキャンの無効化、およびワンタイム プログラマブル) が追加されました。CoolRunner-II のセキュリティについては、**ホワイト ペーパー 265** を参照してください。

まとめ

エンジニアリング、オーバービルディング、クローニングによるセキュリティの侵害は、会社の製品販売の不成立、返品およびテクニカル サポートに多大な利益の損害をもたらします。コストおよび損失は恒久的で回復不可能です。Spartan-3A/3AN/3A DSP プラットフォームはこれらの盗難からのデザインの保護を補助します。Device DNA セキュリティは、1 つの特定のデバイスにデザインを関連付けることで、セキュリティ侵害の発生を防ぎます。Spartan-3AN プラットフォームでは、オンチップ Flash および隠されたビットストリーム コンフィギュレーションを含むデザイン レベルのセキュリティ機能が追加され、あらゆるセキュリティ侵害に対する防御が強化されています

参考資料

ザイリンクスの資料

ザイリンクスが提供する次の資料では、低コストの FPGA およびセキュリティに関するその他の情報をご参照いただけます。

Spartan ファミリのセキュリティ アプリケーションに関する資料

1. UG332 : 『Spartan-3 ジェネレーション コンフィギュレーション ユーザー ガイド』(デザイン保護の詳細情報を記載)
2. WP267 : 『Spartan-3A/3AN/3A DSP FPGA のアドバンスド セキュリティ スキーマ』(Spartan-3A および Spartan-3AN FPGA を使用した、より高度なセキュリティ手法を記載)
3. DS529 : 『Spartan-3A FPGA ファミリ データシート』
4. DS557 : 『Spartan-3AN FPGA ファミリ データシート』
5. DS610 : 『Spartan-3A DSP FPGA ファミリ データシート』
6. WP261 : 『FPGA での IP セキュリティ』
7. XAPP780 : 『Dallas Semiconductor/Maxim DS2432 セキュア EEPROM を使用した FPGA IFF コピー プロテクション』

Virtex ファミリのセキュリティに関するホワイト ペーパー

1. WP155 : 『特定の Virtex-II デバイスでのトリプル DES 暗号方式』
2. WP261 : 『FPGA での IP セキュリティ』

CoolRunner-II のセキュリティに関するアプリケーション ノートおよびホワイト ペーパー

1. XAPP371 : 『CoolRunner-II CPLD ガロア体 GF (2^M) 用乗算器』
2. XAPP374 : 『CryptoBlaze : 8 ビット セキュリティ マイクロコントローラ』
3. WP170 : 『保護されたアプリケーションでの CoolRunner-II CPLD』
4. WP265 : 『CoolRunner-II の向上したセキュリティ機能』

スタータ キット デザイン ボード

http://japan.xilinx.com/products/devboards/index.htm

関連資料

次の資料およびリンクからセキュリティに関する追加情報を入手可能です。

1. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems:

   http://www.cl.cam.ac.uk/~rja14/book.html
2. Anderson, Ross, Mike Bond, Jolyon Clulow, and Sergei Skorobogatov. Cryptographic Processors—A Survey:

   http://www.cl.cam.ac.uk/~mkb23/research/Survey.pdf
3. Schneier, Bruce. Applied Cryptography, John Wiley Sons, 1996

4. Dolan, D. G. Abraham, G. Double, and J. Stevens. Transaction Security System, IBM Systems Journal v. 30, no. 2 (1991), pp. 206-229
5. Health Information Privacy :
   http://www.hhs.gov/ocr/hipaa/
6. その他の政府機関からの情報
   http://www.nist.gov/
   http://csrc.nist.gov/CryptoToolkit/aes/ (AES)
   http://www.itl.nist.gov/fipspubs/fip180-1.htm (SHA)
   http://csrc.nist.gov/cryptval/ (FIPS 140-1、FIPS 140-2)
7. Certicom
   http://www.certicom.com
8. RSA
   http://www.rsa.com/
9. Menezes, A.J., P.C. van Oorschot, and S.A. Vanstone, Handbook of Applied Cryptography, 1996, CRC Press. ウェブ サイト : http://www.cacr.math.uwaterloo.ca/hac/
10. Kerchoffs, Auguste. La cryptographie militaire, Journal des sciences militaires, vol. IX, pp. 5-83, Jan. 1883, pp. 161-191, Feb. 1883.

改訂履歴

次の表に、この資料の改訂履歴を示します。

日付	バージョン	改訂内容
2007/07/24	1.0	初版リリース