

Low-Cost Security Solutions with Spartan-3A and Spartan-3AN Platforms

Spartan-3AとSpartan-3AN が実現する低コスト セキュリティ ソリューション

リバース エンジニアリングや
オーバービルディング、クローニングから
デザインを守る Spartan-3 ファミリの新機能

Maureen Smerdon
Strategic Marketing Manager
Xilinx, Inc.
maureen.smerdon@xilinx.com

飛行機への搭乗から玄関ドアのロック、次世代の回路設計にいたるまで、セキュリティは今や重要な問題となりました。設計者が最も恐れるのは、デザインが盗まれて偽造品が市場に溢れることです。国際模倣対策連合 (International AntiCounterfeiting Coalition) によると、2003 年における米国全体の偽造品による被害額は 2,870 億ドルで、世界中で年間に売られる偽造品の総額、4,560 億ドルの 63% を占めるそうです。

本稿では、低コスト FPGA デザインを保護するため、ザイリンクスがどのようなセキュリティ対策を講じているかを解説します。

セキュリティ上の脅威トップ 3

電子機器のデザインで最も一般的な違法行為は、リバース エンジニアリングです。リバース エンジニアリングとは、デザインを盗んだ人物がオープン市場でより安く販売することを目的に、製品を違法に作り直すことです。リバース エンジニアリングにより、研究開発にまったく資金をかけずに、安いコストで、しかもはるかに短期間で製品化できてしまうのです。

今日、企業の製造委託が進んだことで、オーバービルディング (過剰生産) やクローニング (模造) と呼ばれる新たな違法行為が問題化しています。オーバービルディングとは、委託を受けたメーカーが OEM メーカーの発注量以上の数量を製造することです。その発注量以上の製品は、OEM メーカーの承認を得ずに市場に出回ることになります。

クローニングは、デザインや IP、製品のコピーを作り、同じ、もしくは別のラベルを付け、市場に出すことです。この場合も研究開発費はかかりません。オーバービルディングやクローニングによって作られる製品は、きわめて短時間で市場へ送り出され、流通します。

こうした違法行為により、どれだけの無形資産が失われるか分かりません。リバース エンジニアリング、オーバービルディング、クローニングのいずれも、OEM メーカーにとっては莫大な収益ロスです。そればかりか、返品という形で品質に付随するコストもかかります。これはブランド イメージに悪影響を及ぼすだけでなく、不具合を突き止めて消費者の問題を解決するための RMA (返品不良解析) やテクニカル サポートが増加し、OEM メーカーの最終損益に影響を及ぼす可能性さえあります。また、その製品が正規品か模造品かを最後まで判断でき

ないことも
あるでしょう。
このような損失は永久的で、
回復不可能です。

DeviceDNA を用いたセキュリティ

従来、FPGA はリバース エンジニアリングとクローニングに対する防衛策として、ビットストリームの暗号化を用いてきました。一昔前まではそれで十分対応できましたが、今日のオーバービルディングを防ぐことはできません。

では、設計者はこれら 3 つの違法行為からどのようにデザインを保護すればいいのでしょうか？ ザイリンクスは、デザインをクローニングやオーバービルディング、リバース エンジニアリングから保護するため、DeviceDNA を実装した Spartan™-3A と Spartan-3AN デバイス ファミリを発表しました。

デザイン レベルのセキュリティである DeviceDNA は、デザインと IP、エンベデッド コードを保護します。DeviceDNA は、各デバイスに固有の 57 ビットの ID です。この 57 ビット ID は FPGA の特定工



リアに内蔵されており、ザイリンクスのファクトリで設定され、出荷されます。ID は変更することができません。Spartan-3A および Spartan-3AN FPGA は、各デバイスの出荷時に固有の ID が組み込まれます。

この ID は、設計者がパーソナライズしたアルゴリズムと組み合わせて FPGA に格納されます。アルゴリズムは、基本的に DeviceDNA を用いてどのように結果を作成するかを定義する算式です。結果は外部メモリやフラッシュ メモリなど、任意の場所に格納します。アルゴリズムは設計者しか知らないため、セキュリティの鍵を握るのはこのアルゴリズムです。アルゴリズムは FPGA に格納されますが、第三者にはビットストリームの一部にしか見えません。

Spartan-3A のセキュリティ

Spartan-3A デバイスの場合、デバイスのコンフィギュレーション後、アルゴリズムは DeviceDNA を使用した結果をフラッシュメモリに格納されている結果と照合します。両方の結果が一致するとそのデザインは承認されます。一致しない場合は、機能を制限した形でデザインをセットアップできます。どの程度制限するかは任意に決定できます。

この認証プロセスを日常生活に例えてみましょう。軽食を買うためファスト フードのレストランに立ち寄ると考えてください。手持ちの現金がないため、ATM カード (DeviceDNA) を使うことにします。このカードはあなただけが使えるカードです。注文し、磁気カードを読み取り機に通します。

すると、機械から PIN 番号 (パーソナライズしたアルゴリズム) を入力するよう求められます。システムはあなたが入力した PIN 番号を銀行に格納されている番号と照合します。両方の番号が一致すれば軽食を購入できますが、一致しないと空腹のまま店を出るしかありません。

しかし、もし誰かがあなたの ATM カードを持っていて、PIN 番号を知っていたらどうでしょう。PIN の承認アルゴリズム番号を覚えれば、クローンを作成するのは簡単です。承認アルゴリズムをデザインそのものに組み込んであるのは、そのような理由からです。アルゴリズムはプログラマブル ロジック内の最も機密性の高いエリアに格納されており、コンフィギュレーション オプションは数百万通りに上ります。

Spartan-3AN のセキュリティ

ザイリンクスの新しい不揮発性 FPGA、Spartan-3AN プラットフォームの場合、承認プロセスは Spartan-3A とほぼ同じですが、さらにいくつかの面でセキュリティを強化しています。1 番目は、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、ビットストリームを覗くのがいっそう難しくなります。

2 番目は、DeviceDNA と、フラッシュメモリに記録されているファクトリ フラッシュ ID の 2 つの固有のシリアル番号です。2 つの固有の ID を組み合わせることにより 70 バイト以上のシリアル ナンバーができ、膨大な数のアルゴリズムが可能にな

ることから、認証アルゴリズムを破るにはさらに多くの時間が必要です。このように、デザインが FPGA とフラッシュ ID の両方に関連付けられるようになるわけです。

先ほどの例で言えば、2 つの固有の ID を持つということは、軽食を買うために 2 枚の別々のカードが必要ということです。

3 番目の改善点は、格納されている承認コードです。Spartan-3AN プラットフォームでは、承認コードをオンチップのフラッシュ ユーザー フィールドという、1 回のみプログラミング可能な専用の 64 バイトレジスタに格納できます。これにより、自己完結型の完全なセキュリティ システムが実現されます。外部のインターフェイスやストレージが不要なことから、全体的なセキュリティが高まり、リバース エンジニアリングがいっそう難しくなります。

認証アルゴリズムはユーザーが定義するため、デザイン バジェットを考慮しながら適切なセキュリティ レベルをインプリメントできます。認証アルゴリズムはこのセキュリティ システムにおける重要な鍵でもあります。セキュリティが破られないよう、認証プロセスのどこかを秘密にする必要があります。アルゴリズムが未知であるため、このアルゴリズムがデザイン レベルのセキュリティを確保する鍵となるのです。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ことから、FPGA 内の数百万に及ぶコンフィギュレーション ビットのごく一部のビットになります。これらビットの関係や、アルゴリズムが理解できない限り、膨大な数字にしか見えません。図 1 は、Spartan-3AN

図 1 Spartan-3AN FPGA で可能なセキュリティ セットアップ

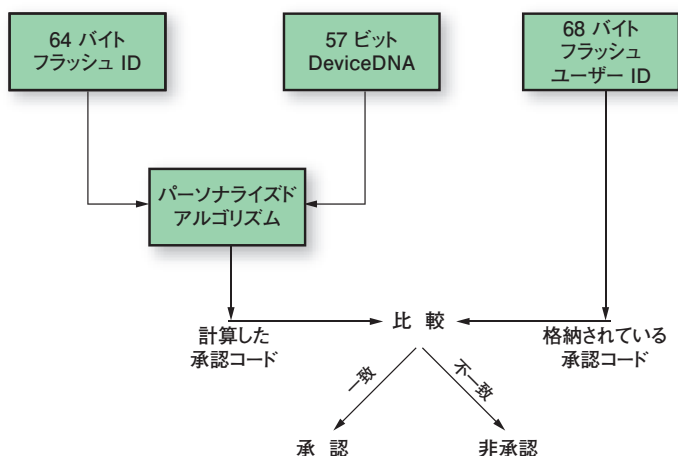
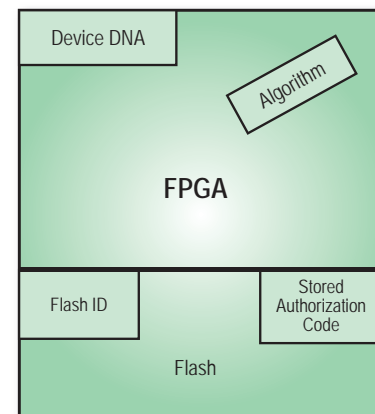


図 2 セキュリティを施した Spartan-3AN デバイス



デバイスで可能な 1 つの流れを示したものです。

図 2 に示す Spartan-3AN のデザインレベル セキュリティは、完全に自己完結型のセキュリティ ソリューションです。フラッシュに、FPGA コンフィギュレーション ビット ストリームと、以前に生成された承認コードが両方格納されています。このコードは、信頼性/セキュリティの保証されたメーカーもしくは登録プロセスにより、一回限りプログラム可能なフラッシュ ユーザー フィールドに格納されます。

電源投入時、FPGA は通常どおりにコンフィギュレーションされます。コンフィギュレーションが終わると、FPGA アプリケーションには、その Spartan-3AN FPGA で動作することを承認されたデザインを有効化するための回路が用意されます。認証アルゴリズムにより DeviceDNA とファクトリ フラッシュ ID が読み込まれ、アクティブな承認コードを生成して、フラッシュ ユーザー フィールドに格納されている以前生成した承認

コードと比較します。両方のコードが同じならデバイスは認証され、異なる場合は不正デバイスとして承認されません。

アクセス拒否

DeviceDNA によるデザイン レベル アプローチのもう 1 つの長所は、失敗した認証の処理方法にあります。認証はデザインに完全に統合できます。したがって、承認されなかったデザインに、次のような複数の対策を取ることができます。

- ・ No functionality – 機能を完全にストップします。
- ・ Limited functionality – 一次回路または主要回路がディスエーブル、もしくはバイパスされます。
- ・ Time bomb – 限られた期間のみすべての機能を利用できます。
- ・ Active defense – システムはアクティビティを監視し、攻撃から防御します。

- ・ Permanent self-destruction – フラッシュの内容をすべて消去し、フラッシュを永久にすべてゼロにします。

これらのデザイン レベルのセキュリティは、Spartan-3A と Spartan-3AN プラットフォーム内で実現可能な基本レベルのセキュリティです。

結論

Spartan-3A および Spartan-3AN プラットフォームのセキュリティ対策は、リバース エンジニアリングやオーバビルディング、クローニングから保護するための数多くの方法を提供します。低コスト FPGA デザインのセキュリティの詳細は、Spartan ジェネレーションのコンフィギュレーション ユーザー ガイド「Spartan-3AN In-System Flash User Guide (英語版)」(<http://japan.xilinx.com/bvdocs/userguides/ug333.pdf>) をご覧ください。

ガイリンクストレーニング スケジュール [11~12月]

9 ~ 10 月のスケジュールは 8 ページをご覧ください。

ガイリンクスでは、大規模、高速 FPGA を対象にした FPGA 設計のための各種トレーニングを各地で開催しております。是非ご利用ください。

コース名	日 程		主 催	開 催 地
ISE デザイン	11 月	1 日 (木)	ガイリンクス	東京会場
	12 月	4 日 (火)	ガイリンクス	東京会場
FPGA 設計導入	11 月	2 日 (金)	ガイリンクス	東京会場
	12 月	5 日 (水)	ガイリンクス	東京会場
FPGA 設計実践	11 月	6 日 (火) ~ 7 日 (水)	アヴネット ジャパン	東京会場
		27 日 (火) ~ 28 日 (水)	ガイリンクス	東京会場
アドバンスド FPGA 設計	12 月	11 日 (火) ~ 12 日 (水)	菱洋エレクトロ	東京会場
	11 月	5 日 (月) ~ 6 日 (火)	新光商事	東京会場
Virtex-4 デザイン	12 月	6 日 (木) ~ 7 日 (金)	ガイリンクス	東京会場
	11 月	15 日 (木) ~ 16 日 (金)	菱洋エレクトロ	大阪会場
Virtex-5 デザイン	12 月	20 日 (木) ~ 21 日 (金)	ガイリンクス	東京会場
	11 月	22 日 (木)	ガイリンクス	東京会場
エンベデッド システム開発	11 月	13 日 (火) ~ 14 日 (水)	PALTEK	東京会場
	12 月	13 日 (木) ~ 14 日 (金)	東京エレクトロデバイス	東京会場
アドバンスド エンベデッド システム開発	11 月	27 日 (火) ~ 28 日 (水)	ガイリンクス	東京会場
	11 月	15 日 (木) ~ 16 日 (金)	東京エレクトロデバイス	東京会場
System Generator を使用した DSP デザイン	12 月	18 日 (火) ~ 19 日 (水)	PALTEK	東京会場
	11 月	29 日 (木) ~ 30 日 (金)	東京エレクトロデバイス	東京会場
MGT シリアル I/O デザイン	12 月	11 日 (火) ~ 12 日 (水)	PALTEK	東京会場

*すべてのトレーニングは、ガイリンクス認定インストラクターによるオフィシャル トレーニングです。

*日程および会場は、都合により変更となる場合もございます。最新情報はガイリンクス トレーニング Web サイトをご覧ください。

詳細とご登録はこちらから ▶▶ <http://japan.xilinx.com/support/education-home.htm>