XAPP1323 (v1.0) 2017 年 10 月 13 日

Zynq UltraScale+ デバイスでの不正操作防止デザインの開発

著者: Ed Peterson

概要

このアプリケーション ノートでは、Zynq® UltraScale+™ デバイスで実現した、システム内に存在する知的所有権 (IP) や機密データを保護する不正操作防止 (AT) の機能について説明し、それらの実例を紹介します。この保護機能 (不正操作防止機能) は、Zynq UltraScale+ デバイスがソフトウェア イメージでセキュア ブートされる間およびその前後、またはプログラマブル ロジック (PL) ビットストリームでコンフィギュレーションされる間およびその前後に有効になっている必要があります。機密データには、デバイス ロジックの機能を設定するソフトウェアやコンフィギュレーション データ、またブート イメージに含まれる重要なデータ/パラメーター (メモリの初期値や初期状態など) があります。起動後の通常動作時に、デバイスに対して動的に書き込みまたは読み出しが実行される外部データも機密データとなります。

ここでは、Zynq UltraScale+ デバイスで利用できるシリコン AT 機能の概要を説明し、これらの機能が必要な理由、各機能の使用例、およびインプリメンテーションの詳細を示します。また、さらなる不正操作防止を実現するための、その他のシステムレベルの方法についても説明します。

このアプリケーション ノートを参考にすることで、Zynq UltraScale+ デバイスで利用できる AT のベスト プラクティスを実現し、ハードウェアの RoT (信頼の基礎) を提供してユーザー アプリケーションを動作させることが可能になります。これらのベスト プラクティスは、商用デザインのクローニングやオーバービルドを防止する目的、軍事システムの重要なクリティカル テクノロジ (CT) のリバース エンジニアリングを防止する目的、またはその中間的な目的で広く適用できます。

このアプリケーション ノートでは、Zynq UltraScale+ デバイスのアーキテクチャ ([参照 1]) とデザイン ([参照 2]、[参照 3]) に関してある程度の知識があり、Vivado® ツールを使用した設計フロー ([参照 4]) の経験があることを前提としています。『Solving Today's Design Security Concerns』(WP365) [参照 5] および『UltraScale FPGA および UltraScale+ FPGA での不正操作防止デザインの開発』(XAPP1098) [参照 6] では、FPGA および SoC におけるさまざまなセキュリティ上の脅威およびソリューションについて説明しています。

はじめに

ザイリンクスは FPGA および SoC (system-on-a-chip) の AT ソリューションにおいて何世代にもわたって業界を牽引してきました。Zynq UltraScale+ デバイスでも、PUF (physical unclonable function)、ユーザー アクセス可能なハードウェアに実装された暗号化ブロック、非対称認証、サイドチャネル攻撃保護、およびその他のシリコンベースの AT 機能を含めることで、信頼性の高いデバイスを提供しています。また、セキュア ブート後のさまざまな不正操作防止機能を提供するために、Security Monitor [参照 7] という IP コアを提供しています。特定の制約によって、Security Monitor の使用には制限があります。詳細は、ザイリンクス販売代理店へお問い合わせください。

不正防止において攻撃者よりも常に一歩リードするということは、継続的なプロセスであり、既存の脆弱性と攻撃を把握して攻撃に対抗するための軽減手法 (対抗措置) を開発する作業が伴います。ザイリンクスは、商用市場と防衛市場の両方を含めた AT 機能を重視するユーザーを対象に、数世代にわたってセキュアな FPGA および SoC 技術を低コストで提供しています。

ザイリンクス FPGA/SoC のさまざまな AT 機能を利用することで、プログラムや顧客要件に基づいてどの程度の AT 機能をデバイス デザインに含めるかを選択できます。個々のシリコン AT 機能を有効にして使用することも、各 AT 機能を組み合わせて使用する (PL デザイン内で AT 機能を組み合わせて、ベスト プラクティスのガイダンスに従うなど) ことも可能です。

主に次の 3 つの要素を考慮して、どの程度の AT 機能を含めるかを判断します。

- 価値: IP の知覚価値および知的所有権が侵害された場合に経済的または国家安全保障に与える損害。特定の AT 機能は実装に高いコストがかかるため、保護対象のテクノロジやデータの価値に対するコストを慎重に検討する必要があります。
- 攻撃者: システムへのアクセス手段および攻撃に伴う専門レベルとリソース。たとえば、システムへのアクセスは「銃、門、警備員」で防ぐことはできるか、一般市場で簡単に入手できるか、攻撃者は個人レベルのハッカーなのか、大規模なグループなのかなど。攻撃者の能力は極端なものから中間レベルに至るまでさまざまです。
- 設計段階: システム開発サイクルのどの段階で Zynq UltraScale+ デバイス デザインに AT を使用すると決定するか。ザイリンクスは、スケジュールとコスト両方の要件を満たすことができるように、Zynq UltraScale+ デバイスの AT 機能の使用に関して可能な限り早期 (システムに CT を定義した直後など) に決定することを強く推奨しています。開発プロセス後の段階で AT 機能を挿入すると必ずコストと時間が増加し、多くの場合効果も低減します。

また、特定の AT 機能を有効にした場合に消費するプロセッシング システム (PS)/プログラマブル ロジック (PL) のリソースも考慮する必要があります。通常、全体的なリソース消費による影響はかなり抑えられますが、機能の実装方法や使用する Zynq UltraScale+ デバイスの相対的な割合によって異なり、大規模なデバイスほど PL リソースへ与える影響は小さくなります。

ザイリンクスでは、シリコンの AT 機能を受動的と能動的に分類しています。一般的に受動的セキュリティ機能はツール フローの一部であるかデバイスに組み込まれているため、PS/PL デザインに対して追加の作業は必要ありません。また、受動的セキュリティ機能は一時的という特性を持ち、Zynq UltraScale+ デバイスの通常の動作サイクルの異なるタイミングで次のような機能を果たします。

- セキュア ブート前 (例: PUF によるブラック キー ストレージ)
- セキュア ブート中 (例: 差分電力解析 (DPA) によるサイドチャネル攻撃の防止)
- セキュア ブート後 (例: PL リードバックの無効化によるユーザー データ保護)

これに対して、能動的セキュリティ機能は PS/PL デザインに含める必要があります。これらの機能は、Zynq UltraScale+ がセキュア ブートされ、デザインがアクティブになった後にのみ有効になります。たとえば、コンフィギュレーション セキュリティ ユニット (CSU) の AES (Advanced Encryption Standard) 制御レジスタに書き込みを実行してバックアップ バッテリ付きの AES キーをゼロ化したり、JTAG トグル検出機能を使用して不正な JTAG イベントに対応する機能などがあります。

最小限の措置として、イメージ/ビットストリームの暗号化や認証などの適切な受動的セキュリティ機能は、デザインに含めるように常に計画する必要があります。これらの機能はデザインの機能性に影響を与えることはありませんが、ロジスティック上の課題 (例: キー管理)、シスム上の課題 (例: キー ストレージ用にバックアップ バッテリ付き RAM (BBRAM) を使用する場合はバッテリが必要)、およびセキュア ブート時間の増加 (例: 公開キー認証によりセキュア ブート時間が増加) などが生じる可能性があります。それ以外では、これらの機能を無償で利用して、相当の改ざん防止策を講じることができます。これらの AT 機能は、ソフトウェアやハードウェア デザインに影響を与えないため、既にフィールド展開されたシステムや開発段階後期のデザインで使用するのに最適です。

このアプリケーション ノートで説明している AT 機能とガイダンスは、主に 3 つの AT カテゴリに分類されます。

- 防止 (例: JTAG ポートのブロック)
- 検出 (例: 電圧および温度の監視)
- 応答 (例: BBRAM キーおよび PL コンフィギュレーションのゼロ化ペナルティ)

表 1 に、Zynq UltraScale+ デバイスのビルトイン シリコン AT 機能の概要とそのカテゴリを示します。

表 1: AT 機能の分類と概要

Zynq UltraScale+ デバイス シリコンの AT 機能	タイプ	カテゴリ	セキュア ブート/ コンフィギュレーション ステージ(1)
イメージ/ビットストリームの機密性 (対称)	受動的	防止	コンフィギュレーション前、 コンフィギュレーション中
揮発性のオンチップ 256 ビット BBRAM AES キー ストレージ	受動的	防止	コンフィギュレーション前
不揮発性のオンチップ 256 ビット eFUSE AES キー ストレージ(3)	受動的	防止	コンフィギュレーション前
PUF によるブロック キー ストレージ (内部 eFUSE または外部フラッシュ ストレージ)(2)	受動的	防止	コンフィギュレーション前

表 1: AT 機能の分類と概要 (続き)

Zynq UltraScale+ デバイス シリコンの AT 機能	タイプ	カテゴリ	セキュア ブート/コンフィギュレーション ステージ[1]
書き込み専用キーの読み込みと整合性チェック (BBRAM および eFUSE)	受動的	防止	コンフィギュレーション前
イメージ/ビットストリームの認証 (対称)	受動的	防止	コンフィギュレーション前、コンフィギュレーション後
イメージ/ビットストリームの認証 (非対称)[2]	受動的	防止	コンフィギュレーション前
RSA 認証を有効化するための不揮発性の 384 ビット eFUSE 公開キー ハッシュ ストレージ[3]	受動的	防止	コンフィギュレーション前
DPA サイドチャネル攻撃からの保護	受動的	防止	コンフィギュレーション中
難読化されたユーザー AES キーの読み込みと格納	受動的	防止	コンフィギュレーション前
ハード化されたリードバック無効化回路	受動的	防止	コンフィギュレーション後
CSU 用の連続した内部クロック ソース	受動的	防止	コンフィギュレーション前、コンフィギュレーション中、コンフィギュレーション後
JTAG ポートの恒久的な無効化 (eFUSE)[3]	受動的または能動的	防止または応答	コンフィギュレーション中、コンフィギュレーション後
JTAG ポートの一時的な無効化	受動的または能動的	防止	コンフィギュレーション中、コンフィギュレーション後
JTAG ポートの監視	能動的	検出	コンフィギュレーション後
PL コンフィギュレーション メモリの整合性チェック	能動的	検出	コンフィギュレーション後
固有識別子 (Device DNA およびユーザー eFUSE)	能動的	検出	コンフィギュレーション後
オンチップ温度および電圧の監視/警告	能動的	検出および応答	コンフィギュレーション中、コンフィギュレーション後
PL コンフィギュレーション メモリの消去	能動的	応答	コンフィギュレーション後
PL STARTUP ブロックの連続した内部クロック ソース	能動的	検出	コンフィギュレーション後
キーの俊敏性 (BBRAM のみ)	能動的	防止および応答	コンフィギュレーション後
BBRAM キーのゼロ化 (消去 + 検証)	能動的	応答	コンフィギュレーション後
CSU の不正操作監視と応答	能動的	検出および応答	コンフィギュレーション後
公開キーの取り消し	能動的	応答	コンフィギュレーション後
不揮発性 (eFUSE) 不正操作イベントのログ記録	能動的	応答	コンフィギュレーション後
ユーザー アクセス可能な暗号化ブロック[2]	能動的	防止	コンフィギュレーション後
ARM® TrustZone	能動的	防止および検出	コンフィギュレーション後
ARM v8 暗号拡張[2]	能動的	防止および検出	コンフィギュレーション後

表 1: AT 機能の分類と概要 (続き)

Zynq UltraScale+ デバイス シリコンの AT 機能	タイプ	カテゴリ	セキュア ブート/コンフィギュレーション ステージ(1)
ザイリンクス メモリ保護ユニット (XMPU)(2)	能動的	防止および検出	コンフィギュレーション後
ザイリンクス ペリフェラル保護ユニット (XPPU)(2)	能動的	防止および検出	コンフィギュレーション後
AXI/APB 分離ブロック (AIB)(2)	能動的	防止および応答	コンフィギュレーション後
システム メモリ管理ユニット (SMMU)(2)	能動的	防止	コンフィギュレーション後
グローバル トライステート (GTS) の有効化 (PL I/O のみ)	能動的	応答	コンフィギュレーション後
グローバル セット/リセット (GST) の有効化 (PL I/O のみ)	能動的	応答	コンフィギュレーション後

注記:

1. Zynq UltraScale+ デバイスの通常動作において、この機能が有効になるときを示しています (セキュア ブート前、セキュア ブート中、セキュア ブート後)。
2. Zynq UltraScale+ デバイスで新たに追加された機能または改善された機能です。
3. 一部の「恒久的な」不正操作防止機能の設定/ペナルティ (eFUSE ベース) のアサートは元に戻すことができないため、デバイスをザイリンクスに返却可能かどうかに影響する可能性があります。

以降のセクションでは前述の機能の仕組みと必要性および適切な使用方法の具体例を挙げながら説明します。これら機能の単独使用、ほかのビルトイン機能やユーザー ロジックと組み合わせて使用、またはこれらの両方の使用方法についても説明します。さらに、Zynq UltraScale+ デバイスのデザインやシステム全体の不正操作防止レベルを強化するために有効な手法やテクニックについても、特定のボード/システム レベルで具体的に説明します。Zynq UltraScale+ デバイスは複雑であるため、これらのセキュリティ機能を実装するための詳細説明は、既存のザイリンクス資料を参照してください。このアプリケーション ノートでは、これらの関連資料/セクションへの参照リンクを提供しています。

Zynq UltraScale+ デバイス レベルで有効な AT 機能は、包括的なシステム レベルの AT ソリューションの一環として考える必要があります。この資料で説明する機能やテクニックは、Zynq UltraScale+ デバイスにとって非常に有効な AT という傘のような機能を果たしますが、AT が効果を最も発揮するのは、常にシステム全体を考慮して多層アプローチで展開された場合です。

Zynq UltraScale+ デバイスのセキュア ブート

信頼できるシステム実現には、電源が投入された瞬間からアプリケーション デザインの実行に至るまでの安全性を確保することが重要です。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「ブートおよびコンフィギュレーション」の章および『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の「システム ブートおよびコンフィギュレーション」の章を参照してください。Zynq UltraScale+ デバイスは、さまざまなセキュリティ機能を提供してブート時のセキュリティを確保します。ハードウェアの RoT (信頼の基礎) を構築するには、ソフトウェア イメージやビットストリームを暗号化し、これらが改ざんされていないことを確認し、信頼できるソース から読み込み開始できるようにする必要があります (ユーザー コードの最初の部分である第 1 段階ブートローダー (FSBL) から読み込み開始)。

図 1 に、セキュア ブート プロセスの一般的な手順を示します。各コンポーネントは変更不可 (例: bootROM コード)、または適切な手順で認証されるトラスト チェーン (信頼の鎖) で管理されています。

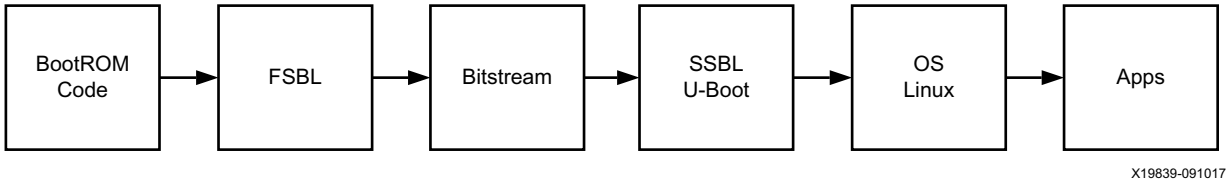

図 1: セキュア ブートのトラスト チェーン

認証プロセスのほかにも、Zynq UltraScale+ デバイスには、クローニング、オーバービルド、リバース エンジニアリングなどの攻撃から保護するためにイメージやビットストリームの機密性を確保する機能があります。また、Zynq UltraScale+ デバイスのセキュア ブート プロセスのロバスト性を強化するために、ブラック キー ストレージやサイドチャネル攻撃対策などのセキュリティ機能が多数あります。

セキュア ブートの概要

Zynq UltraScale+ デバイスには、セキュア ブート プロセスを可能にするための独立したコンフィギュレーション セキュリティ ユニット (CSU) があります。この CSU は低電力ドメイン (LPD) に含まれており、セキュリティおよびブート関連の機能を実行します。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] を参照してください。CSU は、FPGA 内部の連続したクロック ソース (SYSOSC) で駆動されます。

図 2 に示すように、CSU は 2 つの主要ブロックで構成されています。左側には、ブート動作を制御するためのロバスト性の高い三重冗長 MicroBlaze™ プロセッサを含むセキュア プロセッサ ブロック (SPB) があります。また、付属の ROM、小型の専用 RAM、およびすべてのセキュア動作をサポートするために必要な制御/ステータス レジスタもあります。

右側のコンポーネントは暗号インターフェイス ブロック (CIB) で、AES-GCM エンジン、ダイレクト メモリ アクセス (DMA)、SHA (Secure-Hash Algorithm) 関数 SHA-3、RSA アクセラレータ、およびプロセッサ コンフィギュレーション アクセス ポート (PCAP) インターフェイスを備えています。ブート後、CSU を使用して不正操作の監視と応答を実行し、PS または PL のいずれかで動作するアプリケーションが暗号ブロック (AES-GCM、SHA-3、および RSA) へアクセスできるようになります。

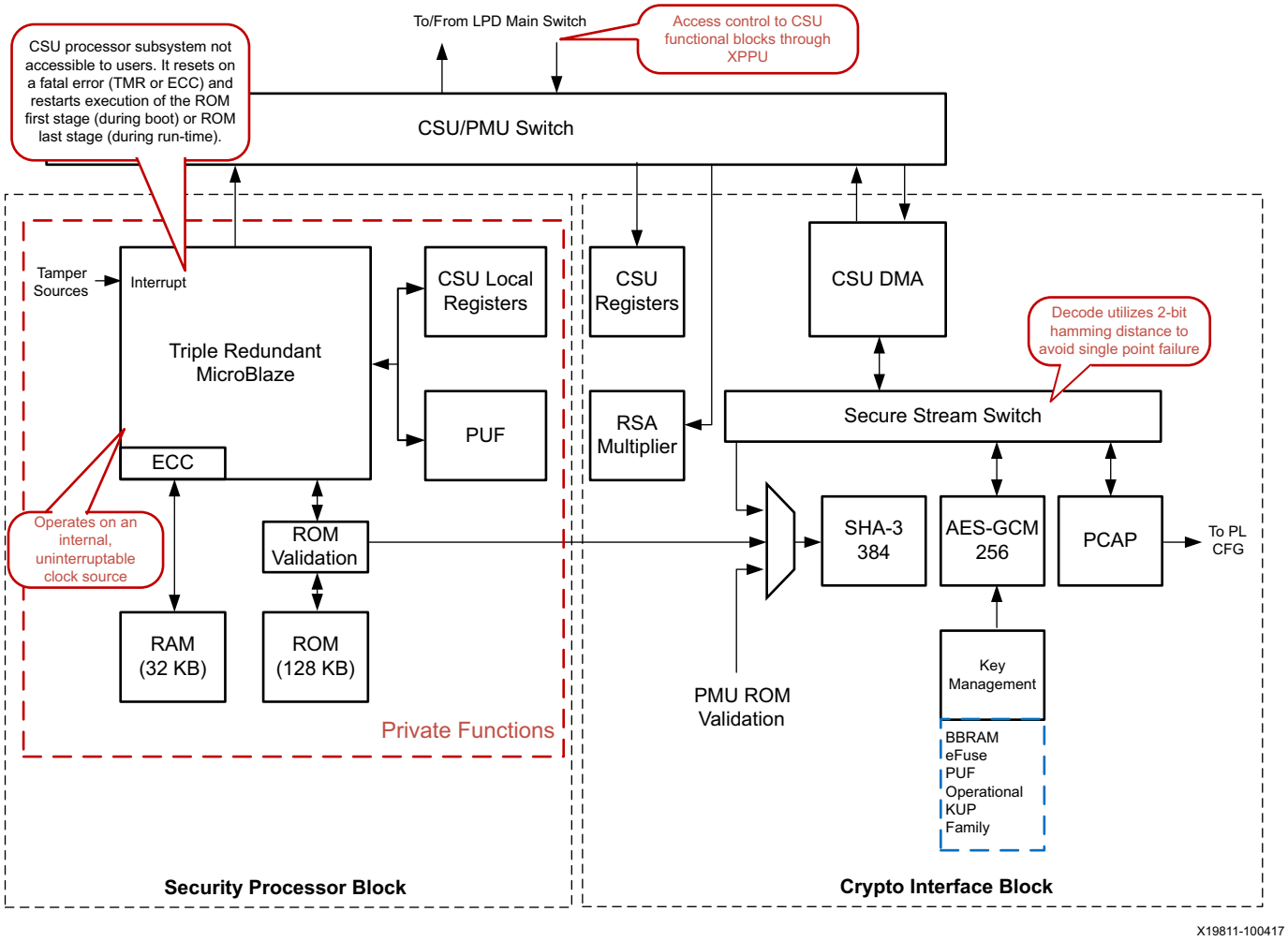

図 2: CSU のブロック図

Zynq UltraScale+ デバイスのセキュア ブート プロセスは、ハードウェア ステート マシンの実行で開始します。ハードウェア ステート マシンがチェック機能とその動作を完了すると、プラットフォーム管理ユニット (PMU) のリセットが解除され、メタル マスクされたブート ROM コードの実行を開始できるようになります (『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] を参照)。CSU と同様に、PMU もロバスト性の高い三重冗長 MicroBlaze プロセッサです。PMU の動作が完了すると、CSU ROM の整合性チェックを実行して、CSU のリセットを解除します。整合性チェックに問題がない場合、CSU は独自のメタル マスクされたブート ROM コードを実行できます。

各機能ユニットで実行される主な機能は次のとおりです (* は、オプション機能)。

1. ハードウェア ステート マシン
   a. インターフェイス ロックダウンのテスト
   b. PMU レジスタのゼロ化
   c. LBIST (Logic Built-In Self-Test) の実行
   d. PMU ROM の SHA-3/384 整合性 チェック
   e. PMU のリセット解放
2. PMU
   a. 低消費電力ドメイン (LPD)/フル電力ドメイン (FPD) レジスタのゼロ化
   b. PMU RAM のゼロ化
   c. 電圧チェック (LPD、AUX、I/O)
   d. CSU、LPD、および FPD のメモリのゼロ化

e. CSU ROM の SHA-3/384 整合性チェック
f. CSU のリセット解放

3. CSU
   a. RSA 認証が有効な場合、ハードウェア (HW) の RoT (信頼の基礎) が強化
   b. セキュリティ ステート (セキュア ブート モード) の強化
   c. ユーザー公開キーの整合性検証
   d. 公開キーの取り消し
   e. 第 1 段階ブートローダー (FSBL) と PMU ユーザー ファームウェア (FW) の読み込み
   f. 認証*/復号化*
   g. 処理後にストレージ エレメントをゼロ化 (フォールバックを含む)
   h. FSBL の実行開始

図 3 に、Zynq UltraScale+ デバイスのセキュア ブート タイムライン を示します。

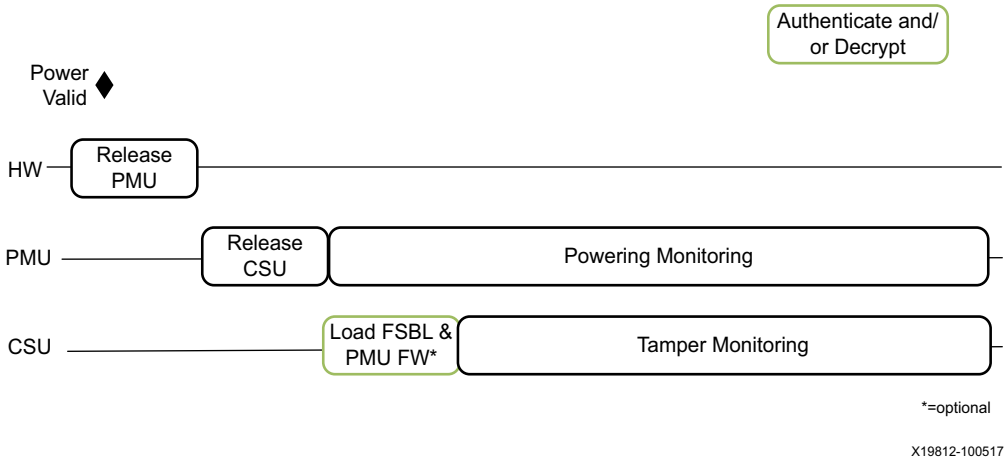

図 3: セキュア ブート タイムライン

セキュア ブート後には、PMU 上で独自のファームウェアを実行して動作をカスタマイズできますが、CSU 上ではユーザー コードを実行できません。CSU 上では、変更不可であるマスクされた ROM コードのみ実行できます。セキュア ブート後、CSU はレジスタ インターフェイスを介して有効化できる不正操作の監視と応答を実行できます。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章および『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG1087) [参照 8] を参照してください。CSU の不正操作監視/応答レジスタ ビットは RWSO (読み出し/書き込み、セットのみ) であるため、一度ビットがセットされると、パワーオン リセット (POR) またはソフト リセット (SRST) されるまでクリアできません。不正な書き込みや悪意のあるソフトウェアによって不正操作応答ペナルティが減ることはなく、ペナルティは増加のみあり得ます。

セキュア ブート プロセス中は、攻撃を受ける可能性が多くあります。Zynq UltraScale+ デバイスでは、ハードウェアの RoT (信頼の基礎) を提供するために、セキュア ブート中にさまざまな対策を講じることができます。表 2 に、これらの攻撃と対策の概要を示します。

表 2: セキュア ブートの保護機能

攻撃	デバイスの対策
サイドチャネル	ビルトインの差分電力解析 (DPA) 機能
グリッチ	CSU/PMU 三重冗長プロセッサ
	CSU/PMU メモリの ECC
	HW および ROM コードの時間的/物理的冗長性
	変更不可の ROM コードで SHA 整合性チェック

表 2: セキュア ブートの保護機能 (続き)

攻撃	デバイスの対策
集束イオンビーム (FIB) プローブ	CSU/PMU 三重冗長プロセッサ
	CSU/PMU メモリの ECC
	HW および ROM コードの時間的/物理的冗長性
	変更不可の ROM コードで SHA 整合性チェック
環境的	内部のランタイム電圧チェック (LPD、AUX、I/O)
	CSU/PMU メモリの ECC
	変更不可の ROM コードで SHA 整合性チェック
テスト インターフェイスの無効化	デザインごと (電源投入時に無効、フォールト トレランス)
	JTAG モニタリング
	恒久的に無効化
一般	変更不可の ROM コード
	PMU/CSU は FPGA 内部の連続したクロック ソースで駆動
	プリブート: 唯一の機密情報は PUF によって保護されるデバイス キー

受動的 AT シリコン機能

イメージ/ビットストリームの機密性と認証 (対称)

暗号化したイメージ/ビットストリームを外部フラッシュなどに格納し、Zynq UltraScale+ デバイスのセキュア ブート中にデバイス内部の復号化エンジンで復号化することで、非常に高レベルの機密性が確保されます。これにより、同じ対称型の秘密キーを共有するユーザーのみがイメージ/ビットストリーム内の情報にアクセスできるようになります。イメージ/ビットストリームの暗号化と復号化により、システムの停止中やセキュア ブート中の機密性が確保され、PL のブロック RAM やフリップフロップの初期化データなどの Zynq UltraScale+ デバイスの PS および PL デザインのコンテンツが保護されます。ザイリンクスでは、外部に格納されるビットストリームは常に暗号化された形式で保持することを強く推奨しています。

注記: Zynq UltraScale+ デバイスでは、NIST (National Institute of Standards and Technology) が認定する Galois/Counter Mode (GCM) の 256 ビット キーの AES を使用しています。ザイリンクス Zynq® UltraScale+ デバイスの AES NIST CAVP 検証に関する投稿は、こちらのサイト (http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#4438) で参照できます。

このセキュリティ機能を利用するにあたり、まず BootGen ソフトウェアを使用してイメージ/ビットストリームを暗号化する必要があります。BootGen はザイリンクスのソフトウェア開発キット (SDK) に含まれておりますが、スタンドアロン ツールとしても提供しています。詳細は、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の「Bootgen イメージの生成」の章を参照してください。BootGen ソフトウェアではユーザーが指定したキーを用いて暗号化が実行されます。AES キーが提供されていない場合は、BootGen ソフトウェアによってオプションで自動的にキーが生成されます。ただし、BootGen ソフトウェアで生成されるキーは疑似ランダムです。真のランダム キーの方がよりセキュアであるため、こちらを強く推奨します。その後、キーは、PS 上で実行されているアプリケーションによって、Zynq UltraScale+ デバイスの BBRAM または eFUSE にロードされます。『SBBRAM および eFUSE のプログラミング』(XAPP1319) [参照 10] を参照してください。

イメージ/ビットストリームの復号化が有効になっている場合、指定された暗号化方法の AES-GCM は認証付きの暗号化/復号化アルゴリズムであるため、対称認証が自動的に有効になります。AES-GCM では、機密性を確保するカウンター モードをユニバーサル ハッシュ (認証タグ) 関数に基づいた認証メカニズムと組み合わせています。そのため AES-GCM では、機密性だけでなく、完全性と認証も同時に実現できます。この暗号化ベースの厳密な認証スキームにより、イメージ/ビットストリームの変更が検出されると、それがシングル ビットであってもデバイスは起動されません。

認証チェックにパスすると、デバイスは通常動作を開始し、スタートアップ コマンドが実行されます。認証ステップをパスしたかどうかは、aes_status レジスタの GCM_TAG_PASS ビットが 1 にセットされていることで確認できます。詳細は、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1085) [参照 2] の 「セキュリティ」の章を参照してください。認証エラーが発生した場合は、イメージ/ビットストリームが不正操作されている可能性が考えられます。イメージ/ビットストリームの読み込みに使用したチャネルがノイズの影響を受け、コンフィギュレーション プロセス中にビットが破損した可能性も考えられます。

揮発性キーおよび不揮発性キーのストレージ

256 ビットの対称 AES-GCM キーは、Zynq UltraScale+ デバイス内の揮発性 BBRAM または不揮発性 eFUSE のいずれかのワンタイム プログラマブル (OTP) ストレージへロードできます。いずれのストレージにキーを格納するかを判断するには、BBRAM (表 3) と eFUSE (表 4) それぞれのストレージの長所と短所を理解しておく必要があります。

表 3: BBRAM ストレージ: 長所と短所

長所	短所
• 揮発性、再プログラム可能 • 受動的および能動的にキーを消去可能 (つまり、証拠を削除できる) • 不正操作防止、物理的なリードバック パスがない	• 外部バッテリが必要 • 多くのバッテリ ベンダーは高温や長期利用における動作仕様を定義していない (一部のベンダーは、これらの問題に対処するために、ベータボルタ式バッテリの提供を開始) • BBRAM にレッド (プレーン テキスト) キーのみ格納できる

表 4: eFUSE ストレージ: 長所と短所

長所	短所
• 外部バッテリが不要 • スプーフィングが困難 (ボード上のデバイスの交換が必要) • レッド (プレーン テキスト) またはブラック (暗号化) 形式でキーを格納できる (「PUF によるブラック キー ストレージ」を参照) • 不正操作防止、物理的なリードバック パスがない	• キーのアップデートが不可 • キーのクリアが不可

PUF によるブラック キー ストレージ

Zynq UltraScale+ デバイスには、ハードウェアに実装された PUF (Physically Uncloneable Function) (Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1085) [参照 2] の 「セキュリティ」の章を参照) があり、デバイス固有のシグネチャやフィンガープリントを生成します。PUF 出力は、同じシリコン ウェハーのデバイスであってもデバイスごとに異なります。Zynq UltraScale+ デバイスと同様、一部の PUF インプリメンテーションでは出力 (応答) がデバイス内でのみ伝達され、製造メーカーを含む他者に公開されることはありません。

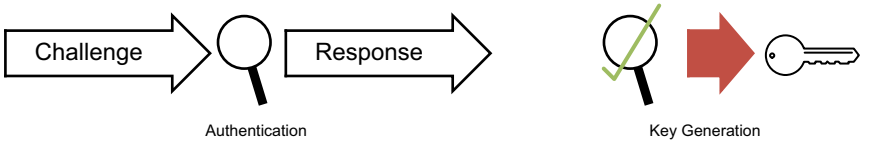

図 4: PUF

PUF は、しきい値電圧、酸化膜の厚さ、金属の形状、抵抗、容量などの、各デバイスのわずかな CMOS 製造プロセスのばらつきを利用します。ザイリンクス デバイスは、これらの通常プロセスの変動内で機能に影響を与えることなく動作するように設計されています。PUF が有効かつ効果的であるためには、環境条件や経年変化の影響を受けることなく、デバイス固有のシグネチャまたはフィンガープリントを正確に再現できることが重要です。

Zynq UltraScale+ デバイスの PUF は、デバイス間の高度なエントロピー (デバイス間のばらつき)、安定性 (デバイス内部の再現性)、およびライフタイムの信頼性を示すために、環境的な極値 (温度や電圧) で加速経年試験を実施して確実に特性評価されています。詳細は、『Zynq UltraScale+ MPSoC PUF Characterization Report』(RPT236) [参照 9] を参照してください。

Zynq UltraScale+ デバイス以前のザイリンクス デバイスの場合、対称 AES-256 キーが BBRAM または不揮発性 eFUSE のいずれかのデバイスに格納されます。このキーは、オンチップの AES 暗号エンジンと連動して、暗号化された FPGA ビットストリームや SoC ソフトウェア イメージを復号化します。オンチップ ストレージはセキュアですが、このキー自体は暗号化されていない (レッド) 状態で格納されるため、物理的攻撃の対象になる可能性があります。

Zynq UltraScale+ デバイスのオンチップ PUF の主な使用例は、KEK (key encryption key) を生成することです。KEK を使用してレッド キーを暗号化してからデバイスの eFUSE に格納することで、暗号化された (ブラック) 形式で安全に格納することが可能になります。攻撃者がオンチップ ストレージ コンテンツにアクセスできたとしても、キーは暗号化されており、有用な情報が含まれていないため、無駄な労力となります。また、キーは暗号化されているため、外部フラッシュに格納することも可能です。詳細は、『SBBRAM および eFUSE のプログラミング』(XAPP1319) [参照 10] および 『Zynq UltraScale+ MPSoC: エンベデッド デザイン チュートリアル』(UG1209) [参照 11] を参照してください。

図 5 は、ユーザー レッド キーの KEK を生成するために Zynq UltraScale+ デバイスの PUF を使用する例を示しています。

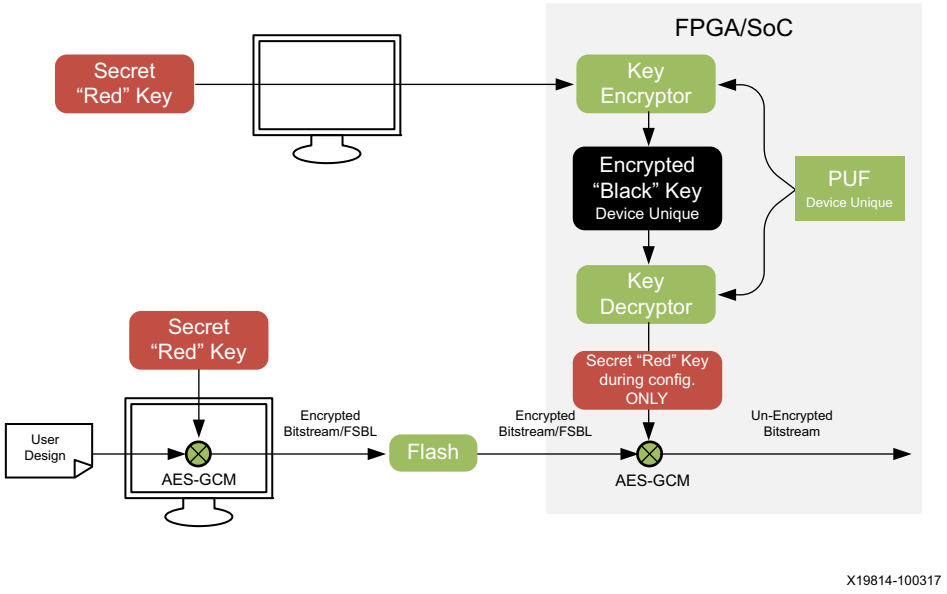

図 5: Zynq UltraScale+ デバイスの PUF 使用例

ユーザーのレッド キーを暗号化してデバイス (eFUSE または外部フラッシュ メモリ) に保存するプロセスのことをプロビジョニングまたはレジストレーションと呼んでいます。『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の付録にある XilSKey ライブラリ (xilskey_puf_registration) を参照してください。フィールド展開する前に、PUF KEK を使用してユーザーのレッド キーを保護するレジストレーション プロセスが実行されます。レジストレーション プロセスでは、4Kb のヘルパー データも作成されます。PUF の再生成プロセスではランダムなノイズが生じるため、電圧、温度、経年変化によるノイズがある場合でも常に PUF の正確な KEK ビットを再生成できるようにヘルパー データが必要です。その後、ラップ (ブラック) キーとヘルパー データは、eFUSE またはフラッシュ メモリなどの外部の不揮発性メモリ (NVM) に格納されます。

注記: PUF で暗号化されたキーは BBRAM に格納できないため、eFUSE または外部フラッシュに格納してください。

デバイスのレジストレーション プロセスが完了し、フィールドに展開された後は PUF を使用して再生成というプロセスが実行されます。基本的に、セキュア ブート プロセスの一環として PUF 回路が KEK ビットを正確に再生成するため、ブラック キーが復号化されてユーザーのレッド キーを取り出すことができます。その後、レッド キーを使用してファームウェア/ビットストリームを復号化すると、すぐにゼロ化されます。この方法の場合、秘密 (レッド) キーは複数プラットフォームに共通で使用できますが、PUF KEK はデバイスごとに固有となるため、固有のブラック値として格納されます。

ブラック キーとヘルパー データがオフチップに格納されている場合は、使用前にデバイスでそれらを常に認証 (RSA-4096 を使用) して差分電力解析 (DPA) やフォールト挿入などの攻撃から保護します。Zynq UltraScale+ デバイスの場

合、PUF は主にセキュア ブート プロセスに使用されます。小規模なユーザー アプリケーション データ (例: ユーザー キー) を暗号化する場合にも使用できます。ユーザー アプリケーション データに使用する場合の詳細は、ザイリンクス FAE へお問い合わせください。

シリコン デバイスに PUF を構成する技術は、アービタ、リング オシレーター (RO)、SRAM メモリなどいくつかありますが、PUF 技術を選択する際には、PUF の有用性について考える必要があります。最も重要なことは、保護される技術のタイプを考えることです。たとえば、SRAM に格納されるキーは、RO ベースの PUF (つまり、非対称技術) を使用して保護することで最大の効果を発揮します。この場合、SRAM ベースの PUF では、SRAM ストレージと同じ攻撃にさらされてしまうからです。Zynq UltraScale+ デバイスの PUF は、RO デザインをベースとしています。

図 6 は、SRAM と eFUSE キーの両方を保護する場合、SRAM ベースの PUF と RO ベースの PUF を比較した場合のこの技術のセキュリティ レベルを表しています。図 6 から、PUF に非対称の技術を使用した場合、攻撃者にとっては複数の技術を打破するスキルが必要となるため、相対的に最い高レベルのセキュリティを実現できることがわかります。

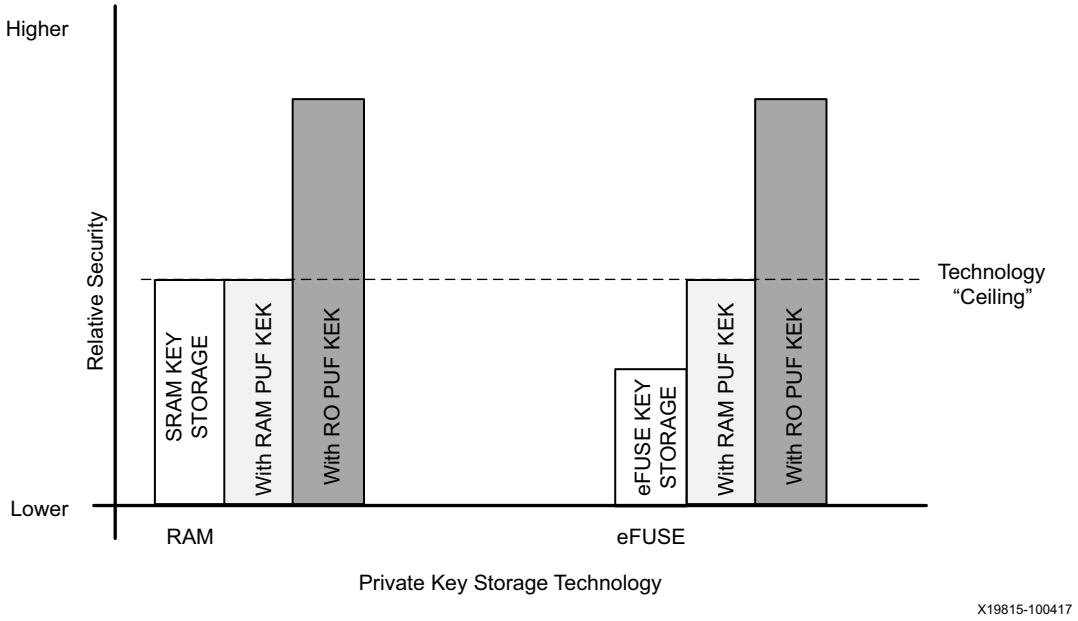

図 6: RAM ベースと RO ベースの PUF 比較

ザイリンクスは、十分なエントロピーを確保するために、さらなるスクリーニングを実行します。エントロピー確保用のスクリーニングのため、ザイリンクスでは 2 つのバージョン (128 ビット、256 ビット) の PUF を提供しています。いずれも実際の KEK 長は 256 ビットです。これらのデバイスを注文する際には特別な注文コード (SCD) が必要です。開発/評価用を除く通常の注文コードでは、PUF 機能がサポートされません 。通常の注文コードの場合、KEK に十分なエントロピーの確保が保証されません。エントロピーの測定については、『Zynq UltraScale+ MPSoC PUF Characterization Report 』(RPT236) [参照 9] を参照してください。PUF を使用する場合に追加ライセンス料金は発生しません。

書き込み専用キーの読み込みと整合性チェック

256 ビットの BBRAM および eFUSE 対称キーは、PS 上で実行されているアプリケーションによって、Zynq UltraScale+ デバイスの BBRAM または eFUSE にロードされます。『SBBRAM および eFUSE のプログラミング』(XAPP1319) [参照 10] を参照してください。Zynq UltraScale+ デバイスの場合、このキーを読み込むパスはデバイスに対して書き込み専用となります。いずれのキーもリードバックするための物理的なデータパスはありません。JTAG または内部パス経由でデバイスにキーが書き込まれる際に、JTAG 経由でデバイスに CRC32 の想定値を書き込むことでキーの整合性チェックが開始されます。実際の CRC32 整合性チェックは、格納されたキーに対してデバイスが (内部で) 算出し、受信した CRC32 の想定値と比較して合/否の結果を生成します。

注記: BBRAM ベースのキーの場合は、キーを書き込む前に、BBRAM にある既存のキーをゼロ化 (消去および検証) してください。

Zynq UltraScale+ デバイスのキー管理

Zynq UltraScale+ デバイスでは、複数のキー ソースやオプションのブラック キー ストレージを利用できるため、従来の FPGA/SoC ファミリよりもキー管理には注意が必要です (図 7)。AES-GCM エンジンを使用する際には、複数あるキー ソースのうちいずれか一つが最初にエンジンへ読み込まれる必要があります。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章、および『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の 「Zynq UltraScale+ MPSoC デバイスのプログラミング ビュー」の章を参照してください。ブート時に CSU の bootROM がキー ソースを選択します。セキュア ブート後、PS 上で動作するソフトウェアがデバイス キーとキー アップデート レジスタ (KUP) のうちいずれかを選択できます。

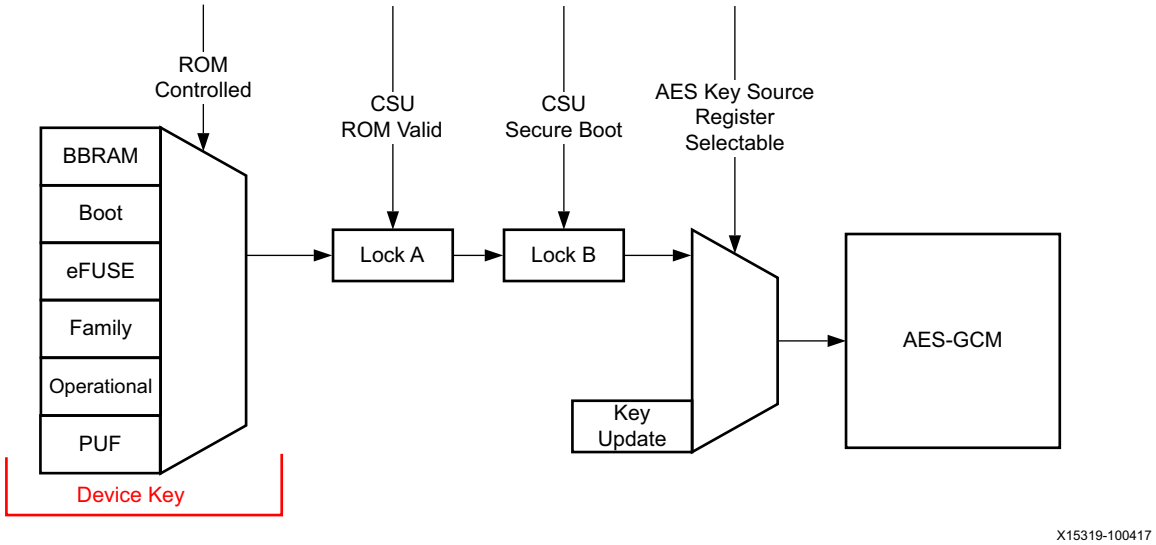

図 7: キー管理

デバイス キー

デバイス キーは、ブート時にブート ヘッダーに基づいて CSU ROM で選択されます。CSU のブート後は、次の POR までデバイス キーのソースを変更できません。デバイス キーは、AES-GCM エンジンがセキュア ブートで使用されている場合、または認証機能が有効になっている場合にのみ利用できます。ブート ヘッダー イメージの属性に Authentication Only Bit が設定され、後で使用できるように CSU ブート ROM にデバイス キーをアンロックするように指示します。非セキュア ブートでは、デバイス キーを利用できません (認証と暗号化のいずれも有効でないため)。デバイス キーの場所は、ブート ヘッダーの Encryption Status フィールドで判断され、下記のいずれかのソースから選択されます。

- BBRAM は 256 ビットのプレーン テキスト (レッド) キーを保持します。
- ブート キー レジスタは、キーが使用されている間、復号化された難読化キーを保持します。
- eFUSE は、256 ビットのプレーン テキスト (レッド) キー、難読化キー、または PUF で暗号化されたキーを保持します。
- ファミリ キーは、デバイスにハードコーディングされた固定の AES キー値です。このキーは、難読化キーを復号化する目的で、CSU ROM の実行中にのみ使用されます。復号化された難読化キーは、ブート イメージの復号化に使用されるプレーン テキスト (レッド) キーです。難読化キーは eFUSE またはブート ヘッダーに格納できます。
- 操作キーを取得するには、ほかのデバイスのキー ソースから得られるプレーン テキスト キーを使用してセキュア ヘッダー (ブロック 0) を復号化します。セキュア ブートの場合、このキーはオプションとなり必須ではありません。操作キーはブート ヘッダーに指定され、デバイス キーの使用を最小限に抑えて露出を制限します。
- PUF キーは、内部の eFUSE キーやフラッシュに格納された外部キーを保護するために使用できる KEK (Key Encryption Key) です。

キー アップデート レジスタ

キー アップデート レジスタ (KUP) は書き込み専用です。このレジスタは、キー ローリング機能のブート時に使用されます。この場合には、異なる AES キーを複数回読み込む必要があります。ブート後は、PS 上で動作しているソフトウェアにより、任意のキーを APB (Advanced Peripheral Bus) を介してこのレジスタに読み込むことができます。256 ビットの KUP キーは、8 つの AES キー アップデート レジスタ (KUP) に格納されます。

イメージ/ビットストリームの認証 (非対称)

Zynq UltraScale+ デバイスには、暗号化/非暗号化イメージ/ビットストリームをオンチップの復号化エンジンに送信する前に、これら全体を認証する機能があります。つまり、認証後の復号化が可能です。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章、および『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の付録で XilRSA ライブラリを参照してください。ビットストリームが変更された場合、それがシングル ビットの場合でも、デバイスの非対称認証機能がこれらの変更を検出し、復号化エンジンを無効にするだけでなく、SEC_LK eFUSE が設定されている場合にはセキュア ロック ダウン モードに遷移してデバイスの起動も阻止します (『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章を参照)。つまり、この機能が有効になっている場合 (RSA_EN eFUSE を使用) は、認可済みイメージ/ビットストリームでのみ Zynq UltraScale+ デバイスのコンフィギュレーションが可能になります。

この方法では RSA-4096 非対称デジタル署名 (認証) アルゴリズムを使用しているため、認証タスク用にデバイスに秘密キーを格納する必要はありません。代わりに、非対称認証機能ではユーザー定義の公開キー情報が使用されます。領域が限られるため、この認証方法では Zynq UltraScale+ デバイスの eFUSE ビットにプログラムされている 4096 ビット公開キーの 384 ビット SHA-3 ハッシュを使用します。必要に応じて、秘密キーと公開キーのペアを定義します。キー ペアは OpenSSL や SafeNet などのさまざまなオープン ソース製品や商用製品を使用して生成できます。この認証方法には、デバイスを動作させるための秘密キーが必要がないため、サイドチャネル解析などの攻撃が発生した場合に、攻撃者に悪用されるような情報は流出しません。

次のような理由から、RSA 非対称認証を使用します。

- 復号化する前に、イメージ/ビットストリーム全体を認証します。この手法は、「DPA の保護」 で説明している DPA 攻撃への対抗措置に含まれています。
- 認可されていないユーザーが、悪意のある可能性がある独自デザインを Zynq UltraScale+ デバイスで実行するのを防ぎます。認可されているユーザーが eFUSE ビットに公開キー ハッシュをプログラムしており、15 の RSA Enable eFUSE のうちいずれかがプログラム (RSA 認証を強制) されている場合は、認可されたイメージ/ビットストリームのみが読み込まれます。
- 暗号化されていないイメージ/ビットストリームの認証。Zynq UltraScale+ デバイスのデザインに機密情報が含まれていなくても、認証が必要な場合があります。次がその例になります。
    - デザインに、AES 暗号化アルゴリズムなどの広く知られている機能が含まれている場合。デザインを機密扱いにする必要はありませんが、たとえば外部ピンなどでレッド キーやデータを出力するなど、変更されないようにする必要があります。
    - Zynq UltraScale+ デバイスのデザインに、基本機能から高度な機能に至るまで、さまざまなレベルの機能が含まれている場合。たとえば、顧客によってアクセスできる機能が異なり、すべての機能にアクセスできる顧客と基本機能にのみアクセスできる顧客がいる場合があります。攻撃者が検知されずに暗号化されていないビットストリームを変更し、拡張機能を試したり、使用することは不可能です。

Zynq UltraScale+ デバイスは、オンチップ eFUSE に 2 つの PPK (プライマリ公開キー) の 384 ビット ハッシュ値を格納できます (フル PPK はブート イメージ内にある)。プライマリ秘密/公開キーの使用を制限するため、PPK はセカンダリ公開キー (SPK) の認証にのみ使用されます。SPK はブート イメージ内に含まれており、残りのブート イメージ/ビットストリームの認証に使用されます。Zynq UltraScale+ デバイスには最大 32 個の SPK を含めることができます。セキュア ブート イメージのフォーマットは、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「ブートおよびコンフィギュレーション」と 「セキュリティ」の章および『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の第 15 章 「Bootgen イメージの生成」を参照してください。

Zynq UltraScale+ デバイスからは、セキュア ブート プロセスに関連する公開キーを無効にする機能が備わっています。2 個の PPK (sec_ctrl eFUSE レジスタ) と 32 個の SPK (spk_id eFUSE レジスタ) を無効化できます。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「セキュリティ」の章および『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG1087) [参照 8] を参照してください。両方の PPK が無効になり、いずれかの RSA_EN eFUSE がプログラムされている場合は、Zynq UltraScale+ デバイスが恒久的に動作できない (ブリック) 状態となり、深刻な不正操作ペナルティとして扱われることがあります。フィールド展開されたシステムの SPK を無効にすると、新しいイメー

ジ/ビットストリームが別の有効なセカンダリ秘密キーでサインされて対応する新しい SPK ID がデバイスにプログラムされるまで、そのデバイスに対して一時的な不正操作ペナルティが作成されます。

すべてのイメージ/ビットストリームは、使用前に認証されます。RSA 非対称認証方法 (暗号化されたイメージ/ビットストリームを使用する場合と使用しない場合) を使用する場合、追加のセキュア ブート/コンフィギュレーション時間が生じます。ザイリンクスは、ブート時間へ与える影響を算出するための Boot Timer Estimator スプレッドシート ツールを提供しています。詳細は、ザイリンクス アンサー レコード 67475 「Zynq UltraScale+ MPSoC - ブート時間の見積もり」[参照 12] を参照してください。

DPA の保護

通常、攻撃者はセキュリティ機能を直接攻撃 (例: 実行不可能なキー総あたり攻撃を使用して Zynq UltraScale+ デバイスのイメージ/ビットストリームの AES-256 復号化を解読) するのではなく、サイドチャネル解析などの比較的簡単な方法を好む傾向があります。サイドチャネルとは、電子デバイス内に存在する想定外の情報流出経路です。観測期間が十分ある場合は、サイドチャネルから暗号化機能のキー データなどの秘密情報を抽出できる可能性があります。

差分電力解析 (DPA) はサイドチャネル技術を使用した攻撃です。機能中の電子デバイスにおける消費電力変化のサンプルを観測して記録し、その後、信号処理と統計手法を用いて記録されたデータから AES-GCM キーを抽出します。攻撃者の能力が向上するにつれ、必要となるサンプル データの数も減少しています。

ザイリンクスは、攻撃者が特定キーに対して収集できるサイドチャネル データ量を制限することで、DPA 耐性を強化しています。このプロトコル ベースのデータ制限手法を Zynq UltraScale+ デバイスで使用することにより、オンチップのビットストリーム復号器の DPA 攻撃から保護します。この手法では、保護レベルがプログラム可能であり、攻撃者の能力が向上するのに伴い保護レベルも強化できるため、長期にわたって最大限の柔軟性が得られます。

その際、無効/ランダムなビットストリーム データと有効なビットストリーム データの 2 種類のデータを制限する必要があります。効果を得るには、これら両方のビットストリームに対する攻撃への対抗措置が必要です。

無効またはランダムなイメージ/ビットストリーム データ

従来、DPA 攻撃者は、大量のランダム データを復号器の暗号化テキスト入力ポートに送り込むだけで、解析用のサイドチャネル情報を収集していました。Zynq UltraScale+ デバイスでは、暗号化されたイメージ/ビットストリームを非対称認証 (RSA-4096) を使用して認証し、このランダム (無効) なイメージ/ビットストリームを検出してから復号器に送信します。シグネチャ検証プロセスに対するサイドチャネル攻撃は、検出するような秘密情報がないため意味がありません (公開キーと公開キー ハッシュは誰でも入手可能)。この方法は eFUSE または BBRAM ベースの AES-GCM キーに使用でき、不正操作ペナルティ (例: キーのゼロ化) は自動的に実行されません。

有効なイメージ/ビットストリーム データ

今日の FPGA および SoC のビットストリーム長は、1 つの有効なイメージ/ビットストリームのロードで DPA 攻撃が実行される十分な長さがあります (入力をさまざまに変化させることで有効なイメージ/ビットストリーム データは十分に不規則になる)。この攻撃から保護するため、Zynq UltraScale+ デバイスのイメージ/ビットストリームは複数の小さなブロックに分割できます。各ブロックは独自のキーを使用して暗号化されます。セキュリティ要件に応じて、各ブロックのサイズをプログラムできます。ブロックのサイズが小さいほど、各キーのサイドチャネル データが少なくなるため、セキュリティが向上します。ただし、小さすぎるとブート時間が長くなる可能性があります。

オンチップ メモリ (BBRAM または eFUSE) にすべての復号化キーを格納せずに済むように、Zynq UltraScale+ デバイスでは、キー ローリング手法が使用され、最初のキー (key 0) のみがオンチップに格納されます。後続の各ブロックのキーは前のブロック内で暗号化 (ラップ) されます。図 8 にこの概念を示します。

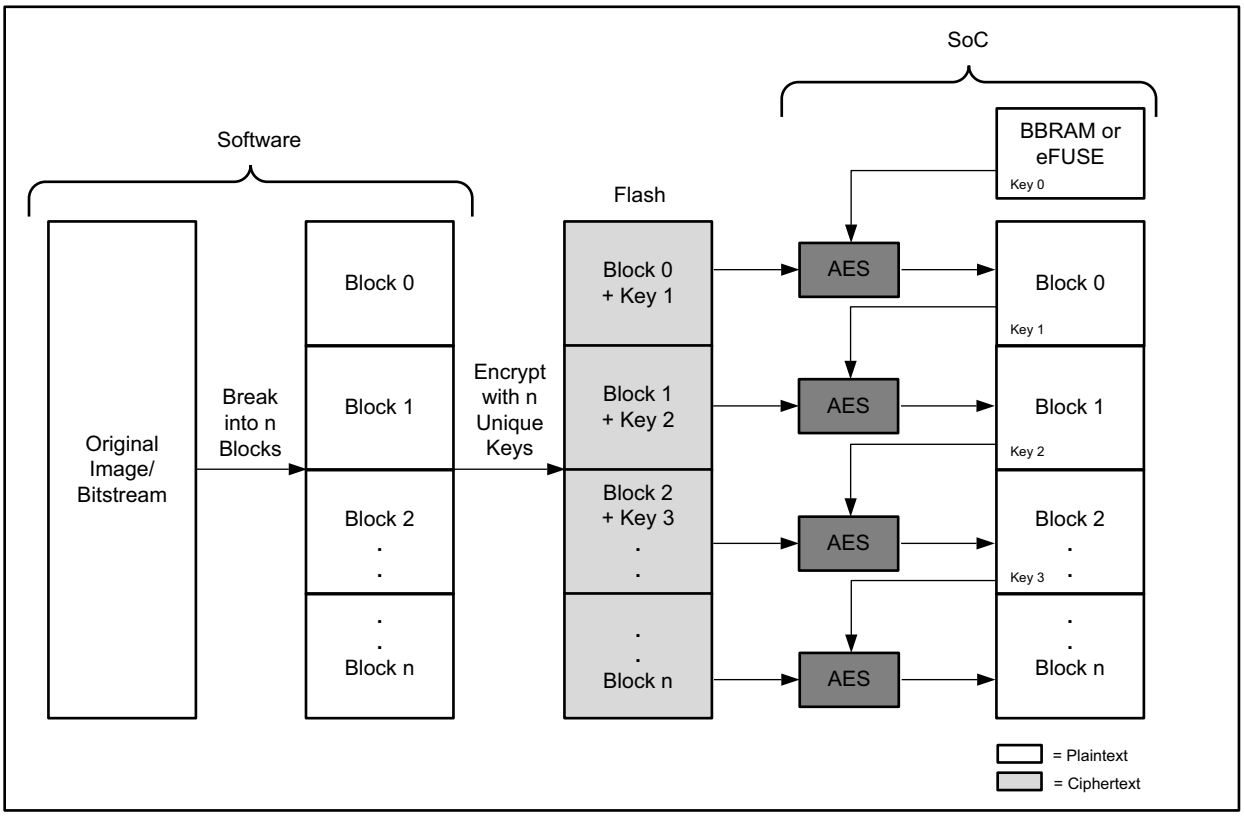

図 8: キー ローリング

有効なイメージ/ビットストリームを何度でも無制限にロードすることは可能ですが、さらなるコンフィギュレーションにより新たなサイド チャネル情報が攻撃者に流出することはありません。攻撃者が実行できるのは、最初のコンフィギュレーションに含まれているサイド チャネル データの信号対ノイズ比を低減させることだけです。キー ローリング手法を認証後復号化と併用すると、攻撃者が暗号化テキスト ポートに適用する値を取得することはできません。

重要: キー ローリング (有効データ攻撃への対抗措置) をランダム データ攻撃への対抗措置 (認証後復号化) と併用する必要があります。

難読化キーの読み込みとストレージ

必要に応じて、Zynq UltraScale+ デバイスの eFUSE アレイに書き込まれて格納されたキー データを難読化できます。キー データは、ザイリンクスのみが把握し、すべての Zynq UltraScale+ デバイスに共通する固定のファミリー キーを使用して暗号化されます(Zynq UltraScale+ デバイスのファミリー キーは UltraScale+ FPGA デバイスのファミリー キーとは異なる)。これにより、委託製造メーカーにおける秘密のレッド キーの保護など、商用量産時のセキュリティ レベルが強化されます。内部に格納された難読化キーは、暗号化されたイメージ/ビットストリームの読み込み開始時に解読され、その後、イメージ/ビットストリームの復号化に使用されます。この機能は、ブート ヘッダーで有効です。図 9 に、この動作の概要を示します。詳細は、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1085) [参照 2] の 「ブートおよびコンフィギュレーション」および 「セキュリティ」の章を参照してください。

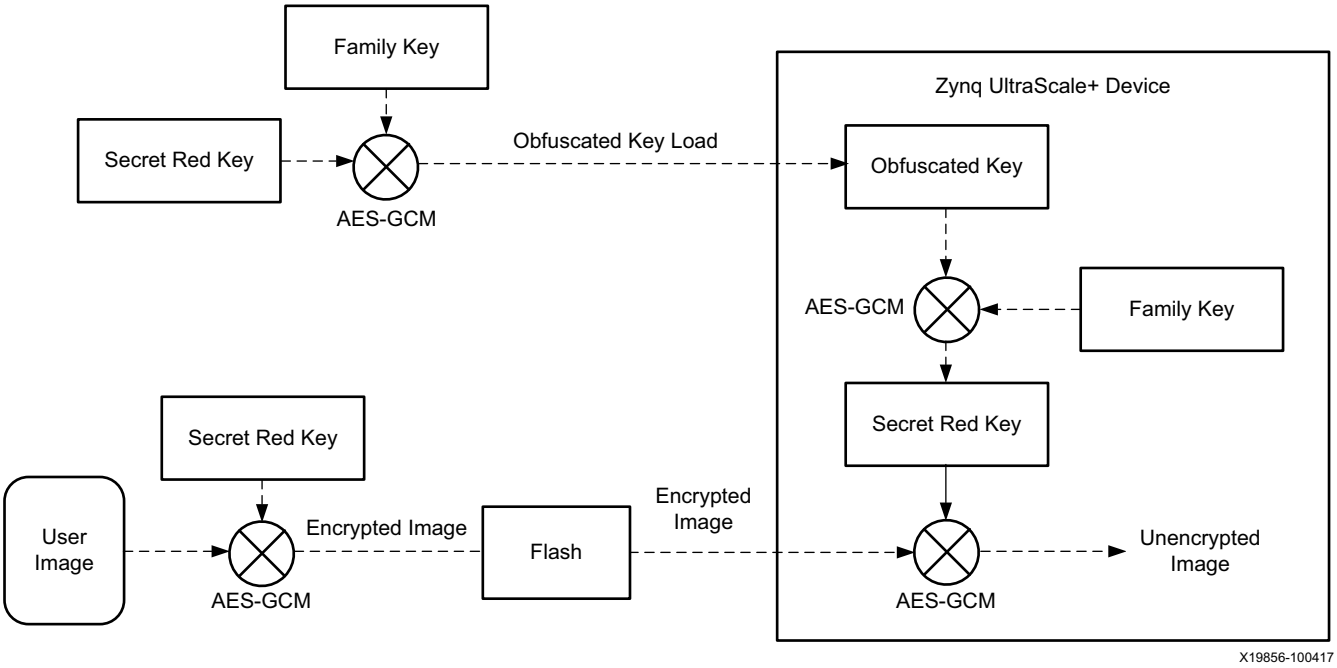

図 9: 難読化キーの読み込みとストレージの概要

ハード化されたリードバック無効化回路

暗号化されたビットストリームまたは認証されたビットストリームが Zynq UltraScale+ デバイスにロードされた場合、JTAG をはじめとする外部インターフェイスによる内部 PL コンフィギュレーション メモリのリードバックは一切実行できなくなります。多層分散により、すべての外部リードバックが自動的にブロック (無効化) されます。暗号化されたビットストリームをロードした後にコンフィギュレーション メモリをリードバックする場合、PS のプロセッサ コンフィギュレーション アクセス ポート (PCAP) または PL の内部コンフィギュレーション アクセス ポート (ICAP) を介してのみ可能です。PCAP へのアクセスは、PS 上で動作する認証済みソフトウェアで制御されるため、信頼できるチャネルと見なすことができます。ICAP についても、PL ビットストリームは読み込みプロセス中に認証され、PL 内のデザインに直接接続されている場合のみ使用可能であるため、信頼できるチャネルと見なすことができます。PL デザインに ICAP がインスタンシエートされていない場合は一切使用できません。PL ロジックを通って ICAP とユーザー I/O 間が直接接続されている場合は信頼できないチャネルと見なされるため推奨されていません。

JTAG ポートの無効化 (受動的)

SEC_CTRL eFUSE レジスタの JTAG_DIS eFUSE ビットをプログラムすると、JTAG コントローラーを恒久的に無効にできます。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「システム テストおよびデバッグ」の章および 『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG1087) [参照 8] を参照してください。eFUSE がブロー (プログラム) されている場合、JTAG は 2 つのコマンド (IDCODE および BYPASS) に限定されます。IDCODE は、JTAG コントローラーをリセットした場合にのみ有効になります (Test-Logic-Reset ステートへ遷移)。命令レジスタ (IR) にシフトされるすべてのコマンドは BYPASS に変換されます。また、JTAG 無効化の eFUSE がブローされている場合、すべてのセキュリティ ゲートが恒久的に有効になるため、Zynq UltraScale+ デバイスのテスト アクセス ポート (TAP) や ARM コアのデバッグ アクセス ポート (DAP) へはアクセスできなくなります。

- IDCODE は、JTAG が Test-Logic-Reset ステートへ遷移すると有効になります。
- BYPASS は、ほかの命令を IR にシフトすることで有効になります。
- すべてのセキュリティ ゲートが恒久的に有効になります。

セキュリティ関連 eFUSE

Zynq UltraScale+ デバイスには、ブラック AES キーやヘルパー データ、レッド AES キー、プライマリ公開キー ハッシュ、セカンダリ公開キー ID を格納しているため、不正操作を記録するためのセキュリティ関連 eFUSE が多数あります。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章にある「Tamper and Monitor Registers」の表および 『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG1087) [参照 8] を参照してください。

能動的 AT シリコン機能

「はじめに」で説明したように、能動的 AT 機能を活用するには PS コードや PL ロジック デザインに手を加える必要があります。たとえば、何らかの不正操作イベントに応答して、いずれかの PS プロセッサで動作するアプリケーションを介して CSU AES 制御レジスタの aes_key_clear ビットにロジック 1 を書き込むことができます (『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章を参照)。表 5 に、これらの能動的 AT 機能、使用例、および実装方法について概要を示します。

表 5: 能動的セキュリティ機能の使用例

機能	使用例	方法
JTAG ポートの恒久的な無効化 (eFUSE)	不正操作イベントに応答して不正な JTAG アクセスを恒久的に防止します。	sec_ctrl eFUSE レジスタの jtag_dis eFUSE ビットを動的にプログラムします。
JTAG ポートの一時的な無効化	不正な JTAG アクセスを防止します。	デバイスを安全に起動します (デフォルトで JTAG は無効)。
JTAG ポートの監視	不正な JTAG アクセスを検出します。	対応する csu_tamper レジスタで JTAG トグル検出機能を有効にします。
コンフィギュレーション メモリの整合性チェック	コンフィギュレーション メモリの整合性をバックグラウンドでチェックします (干渉なしのランタイム チェック)。	Soft Error Mitigation (SEM) IP コアをインスタンシエートします [参照 13]。
固有識別子 (Device DNA およびユーザー eFUSE)	固有識別子が認識されない場合、デザインの動作を不可にするか、制限付きで動作可能にします。	固有識別子を読み出して処理し、それらが有効かどうかを判断できる PS コードまたは PL ロジックを構築します。
オンチップ温度および電圧の監視/警告	通常の環境範囲内でデバイスが動作していることを確認します。	システム モニター (SYSMON) プリミティブをインスタンシエートし、環境状態をチェック/応答する PS コードまたは PL ロジックを構築します (『UltraScale アーキテクチャ システム モニター ユーザー ガイド』(UG580) [参照 15] を参照)。
連続した内部クロック ソース	外部クロック ソースを削除するだけでは、能動的 AT 機能が無効化されないようにします。	STARTUP プリミティブをインスタンシエートし、CFGMCLK 出力に接続して、ユーザー定義の AT 機能のクロック ソースとして使用します (『UltraScale アーキテクチャ ライブラリ ガイド』(UG974) [参照 14] を参照)。
PL コンフィギュレーション メモリの消去	不正操作イベントに応答してコンフィギュレーション メモリを消去します。	PCAP を介す IPROG コマンド送信の適切な条件を決定する PS コードを構築します。
キーの俊敏性 (BBRAM のみ)	ボードやモジュールをセキュアな施設に戻さずに BBRAM キーをフィールドで安全にアップデートします。	キー管理イベントに応答してロジックでセキュアなキー交換を実行し、PS を介して新しい BBRAM キーを読み込むことができる PS コードまたは PL ロジックを構築します。
BBRAM キーのゼロ化 (消去 + 検証)	不正操作イベントに応答してバックアップ バッテリ付きキーをゼロ化します。	aes_key_clear レジスタを介す AES キー消去の適切な条件、および aes_status レジスタの検証ビット読み出しの適切な条件を決定する PS コードを構築します。
CSU の不正操作の監視と応答(1)	セキュリティに不可欠となるさまざまなデバイス パラメーター (電圧、温度) を監視し、適切な不正操作ペナルティをアサートします。	CSU の不正操作/応答レジスタが必要に応じてシステムで設定される PS コードを構築します。
公開キーの取り消し(1)	セキュリティ違反や通常の暗号化有効期間のアップデートが原因となるキー管理イベントに応答して、プライマリ公開キー (PPK) またはセカンダリ公開キー (SPK) を無効にします。	期限切れの PKK または SPK を無効にする PS コードを構築します。

表 5: 能動的セキュリティ機能の使用例 (続き)

機能	使用例	方法
不揮発性 (eFUSE) 不正操作イベントのログ記録(1)	以降のフォレンジック分析に備えて、不正操作イベントを不揮発性メモリ (eFUSE) に安全に記録します。	USER_7 eFUSE レジスタを使用して USER_0 に不正操作イベントを記録する PS コードを構築します。
ユーザー アクセス可能な暗号化ブロック(1)	セキュアブート後に、ハードウェアに実装された AES-GCM、RSA、または SHA の暗号アクセラレータにアクセスして使用します。	アプリケーションで使用されることを目的として、暗号アクセラレータとインターフェイスする PS コードまたは PL ロジックを構築します。
ARM TrustZone	1 つのシステム内でセキュアなプロセスと非セキュアなプロセスを分離して管理します。	PS コードを構築、または ARM TrustZone の機能を利用するオペレーティング システムを使用します。
ARM v8 暗号拡張(1)	ARM PS アプリケーションが AES、SHA、および有限体演算の暗号アクセラレータ命令を呼び出すことを可能にします。	PS コードを構築、または ARM v8 暗号拡張機能を利用するオペレーティング システムを使用します。
メモリ保護ユニット (XMPU)(1)	メモリとフルパワードメイン (FPD) スレーブに対してメモリを分割し、保護する機能を提供します。	Vivado Design Suite のプロセッシング システム コンフィギュレーション ウィザード (PCW) を使用して、XMPU ブロックを設定、または PS 上で実行するコードを使用します。
ペリフェラル保護ユニット (XPPU)(1)	低電力ドメイン (LPD) ペリフェラルを分離し、IP インテグレーターで保護する機能を提供します。	Vivado Design Suite PCW を使用して、XPPU ブロックを設定、または PS 上で実行するコードを使用します。
AXI/APB 分離ブロック (AIB)(1)	AXI/APB マスターとスレーブを機能的に分離します。	Vivado Design Suite の PCW を使用して、AIB ブロックを設定、または PS 上で実行するコードを使用します。
システム メモリ管理ユニット (SMMU)(1)	CPU 以外の任意の DMA 対応エージェントに対するアドレス変換と分離の機能をサポートします。	Vivado Design Suite の PCW を使用して、SMMU ブロックを設定、または PS 上で実行するコードを使用します。
GTS	不正操作イベントに応答して出力を遮断し、デバイスからの情報流出を防ぎます。	セキュア ロックダウンやすべての GPIO をトライステートにするための CSU 不正操作応答を設定する PS コードを構築するか、PL に STARTUP プリミティブをインスタンシエートして、GTS アサートの正しい条件を決定する PL ロジックを構築します。
GSR	不正操作イベントに応答して PL のフリップフロップ ステートを初期状態に戻し、デバイス内の考えられる CT を効率的に消去します。	STARTUP プリミティブをインスタンシエートし、GSR アサートの正しい条件を決定する PL ロジックを構築します。

注記:

1. Zynq UltraScale+ デバイスで新たに追加された機能または改善された機能です。

JTAG ポートの無効化 (能動的)

通常、攻撃者はシステムへ侵入しようとするとき、まず外部 JTAG ポートを狙います。Zynq UltraScale+ デバイスでは、JTAG ポートをブロックするための能動的な方法が複数用意されており、JTAG ポートを一時的 (レジスタ設定を使用) にも恒久的 (eFUSE を使用) にもブロックできできます。

デフォルトでは、JTAG ポートは無効に設定されており、非セキュア ブート モードが検出された場合や認証済みソフトウェアによるセキュア ブート完了後にのみ有効になります。tag_sec レジスタのビットを使用してセキュリティ ゲートを有効化/無効化し JTAG パスを制御します (このビットはデフォルトで有効)。

Zynq UltraScale+ デバイスのロジック デザインに、専用の外部 JTAG ポートに接続された JTAG ベースのデバッグ ツールがある場合、JTAG チェーンを切断すると、これらのツールが機能しなくなります。Zynq UltraScale+ デバイスのデバック段階では JTAG チェーンを保持し、以降の開発サイクルで JTAG ベースのデバッグ ツールが必要なくなったときにこれを切断できます。

JTAG の監視 (検出)

JTAG トグル検出は、JTAG 信号がトグルしたときに CSU の不正操作応答をトリガーするセキュリティ機能です。テスト データ入力 (TDI) またはテスト モード セレクト (TMS) がアサートされており、テスト クロック (TCK) が動作している場合、トグル検出機能によって CSU にアラートが送信されます。このアラートは、POR 信号を受信するまでアサートされたままとなります。CSU へのアラート送信には、TCK の 3 周期分が必要です。これはアラートの誤検出を防ぐもので、ボードに電源が投入されたり、その他の好ましくない状況を招くことを防止します。

不正操作応答は、CSU の不正操作レジスタが設定されている場合にのみ CSU ROM によって処理されます。いずれかの JTAG セキュリティ ゲートが無効になっている場合、CSU の JTAG トグル検出機能は無効になります。これにより、セキュアなソフトウェアにビルトインのデバッグ モードを備えることができます (システム IRQ が、不正操作応答レジスタにプログラムされる最高レベルの応答であるとする)。

PL コンフィギュレーション メモリの整合性チェック (検出)

復号化されたビットストリームでコンフィギュレーションされた PL の内部コンフィギュレーション メモリ セルが破損していると、Zynq UltraScale+ デバイスが予期しない不正な動作をする可能性があります。このような破損は、コンフィギュレーション後の意図的な不正操作攻撃や、シングル イベント アップセット (SEU) などの意図しないイベントが原因で発生する可能性があります。SEM IP コア [参照 13] を使用すると、デザインのバックグランドでコンフィギュレーション データを継続的にリードバックしてビット反転を検出できます。SEM IP コアを使用すると、SEU の訂正も可能です。

固有識別子 (検出)

固有識別子 (UI) には、Device DNA とユーザー eFUSE の 2 種類あります。これらの UI をクローニング防止セキュリティ対策 (ユーザーのイメージ/ビットストリームを盗用して自分のデバイスをプログラムする行為への対策) として使用したり、UI の値に基づいて特定の機能を有効化または無効化 (アップグレードまたはダウングレード) するために使用できます。

Device DNA は 96 ビットのデバイス固有のシリアル番号で構成され、製造過程で Zynq UltraScale+ デバイス上のワンタイム プログラマブル (OTP) eFUSE ビットにザイリンクスが設定します。ユーザー eFUSE にはユーザーが読み出し/書き込み可能な 256 ビットの OTP 領域があり、PS 上で動作するコードを使用してユーザーが内部で設定できます。『SBBRAM および eFUSE のプログラミング』(XAPP1319) [参照 10] を参照してください。セキュリティ上の目的に合わせて、これらの両方の UI を個別に使用することも、併用することも可能です。

注記: Device DNA またはユーザー eFUSE を使用する場合、固有の ID を持つことになりますが、暗号化のように高い機密性や認証機能 (AES-GCM など) は提供されません。クローニング対策には AES-GCM 暗号化が推奨されます。その上にこれらの UI を利用すれば、AT 全体にもう一重のセキュリティを追加できます。

これらの UI を使用して、イメージ/ビットストリームを 1 つのデバイス (Device DNA の場合) または複数のデバイス (ユーザー eFUSE の場合) に関連付けられます。ユーザーが Zynq UltraScale+ デバイスの PS または PL デザインに UI の比較機能を構築し、この比較結果を用いて Zynq UltraScale+ デバイスの動作を制御できます。たとえば、UI 比較でエラーが発生した場合にデザインの機能を停止あるいは制限できます。UI の使用例を次に示します。

1. セットアップ: 図 10 に示すように、PS/PL デザインから UI 値を読み出し、堅牢な一方向関数 (HMAC や CMAC などのキー タイプ型関数が最も安全) を使用してデバイスへアクセスできるフラッシュ デバイスに格納します。

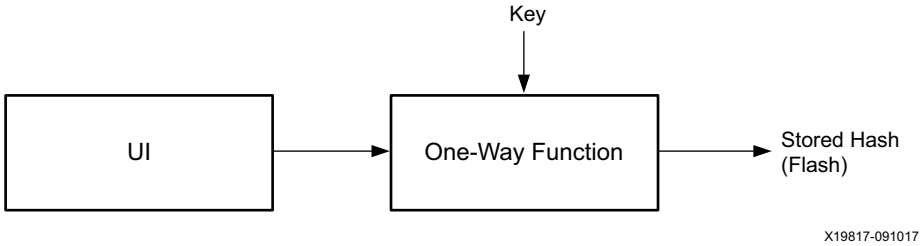

図 10: 秘密キーを使用した DNA 値の暗号化

図 10 に示す一方向関数のキーを、暗号化されたイメージ/ビットストリーム内に格納できます。イメージ/ビットストリーム暗号化を使用しない場合、この方法でハッシュ キーの機密性を確保するには、イメージ/ビットストリームを複雑化する必要があります。

2. Zynq UltraScale+ デバイスを安全に起動します。
3. 比較: まず、Zynq UltraScale+ デバイスの PS コードは、DNA_0 から DNA_2 レジスタまでの UI 値を読み出し (『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1087) [参照 8] を参照)、同じアルゴリズムを使用してハッシュ値を計算します (図 11 を参照)。その後、計算されたハッシュ値とフラッシュから読み出したハッシュを比較します。ハッシュ値が一致するとデザインの動作が許可されます。

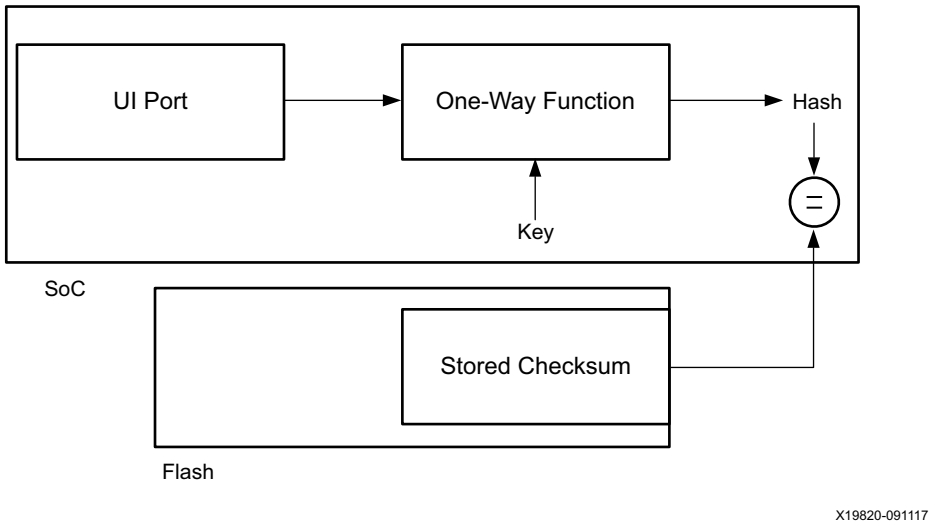

図 11: ハッシュの比較

これらの UI 値に関する詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1087) [参照 8] 、および『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』(WP266) [参照 16] を参照してください。WP266 では、Spartan®-3 ジェネレーション FPGA での Device DNA についても説明しています。

オンチップ温度および電圧の監視/警告 (検出/応答)

攻撃者は、FPGA または SoC の通常動作時の電圧や温度を変更してデバイスに想定外の動作をさせることで、デバイスからデータを抽出したり、特定のセキュリティ機能を迂回するように仕掛ける可能性があります。たとえば、『Federal Information Processing Standards Publication (FIPS) 140-2 Security Requirements For Cryptographic Modules』[参照 17] (暗号化モジュールに関するセキュリティ要件) には、「特に、暗号化モジュールは、指定された通常動作範囲外の動作温度や電圧の変動を監視し、適切に対応する必要がある」と規定されています。

このような要件を満たすために、Zynq UltraScale+ デバイスの PS と PL にはシステム モニター (SYSMON) ブロックが 1 つずつ備えられています。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「PS システム モニター」の章および『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG580) [参照 15] を参照してください。SYSMON ブロックは、ブロックの設定に使用できるレジスタ インターフェイスを備えており、オンチップ電圧とジャンクション温度をモニターする機能を提供します。PL の SYSMON ブロックは、オフチップ電圧を監視できます。また、アラーム生成ロジックがあり、指定されたアラーム条件に基づいてプロセッサに割り込みをかけます。たとえば、

SYSMON ブロックから生成される過剰温度 (OT) アラームに従ってシステムがシャットダウンされたり、内部電圧レールの 1 つが許容範囲を外れると不正操作ペナルティがアサートされたりします。

また、SYSMON には外部基準電圧または内部基準電圧 (VREF) を使用できるオプションもあります。外部基準電圧の方が高精度ですが、内部基準電圧は攻撃者による不正操作が非常に難しいため、内部基準電圧の方が安全です。内部基準電圧と外部基準電圧の選択は外部ピンで制御されます。内部 VREFF が使用されていることを確証するには、適切な SYSMON ステータス レジスタを読み出す必要があります。詳細は、『UltraScale アーキテクチャ システム モニター ユーザー ガイド』(UG580) [参照 15] を参照してください。

オンチップのパラメーターを監視する SYSMON にはアラームの上限と下限を直接プログラムできます。さらに、PL ロジックを使用して、外部アナログ電圧不正操作ループや電圧センサーの出力といった外部電圧入力のアラームの制限値を作成できます。警告信号のステータスをデザインまたはシステムで使用して、これらの信号がアクティブになった場合に実行する適切な一連の動作 (適切な不正操作ペナルティを特定するなど) を判断できます。アナログ入力は帯域幅に制限があります。最大入力周波数は、『UltraScale アーキテクチャ システム モニター ユーザー ガイド』(UG580) [参照 15] を参照してください。

温度や電圧の急な変化を検出する必要がある場合には、オフチップ ソリューションが必要になる可能性があります。検出に必要な帯域幅はシステム設計者が定義します。『Sorcerer's Apprentice Guide to Fault Attacks』[参照 18] では、チップを攻撃するさまざまな手法を説明しており、その 1 つに電源電圧の変動があります。

連続した内部クロック ソース (検出)

ビットストリームの暗号化を使用する場合、PL STARTUP ブロック プリミティブの出力となっている連続したクロック ソース CFGMCLK (コンフィギュレーション内部オシレーター クロック出力) を利用できます。このクロックは常にアクティブであるため、ユーザー クロックまたはその他の重要なユーザー信号の監視機能のベースとして使用できます。CFGMCLK は公称値 50MHz ± 15% (『ZynqUltraScale+ MPSoC データシート : DC 特性および AC スイッチ特性』(DS925) [参照 19] を参照) から変動する可能性がありますが、重要なユーザー クロックやユーザー信号が有効な動作を続け、下限と上限の周波数範囲内でトグルしている (CFGMCLK の変動を考慮) ことを監視する上で非常に有効です。重要なユーザー クロックやユーザー信号がこの範囲から外れた場合は、デザインが誤動作したか不正操作された可能性があり、適切な対策を講じることができます。

CFGMCLK は、PL 内のその他のユーザー定義 AT 機能のクロック ソースとしても使用できます。外部クロック ソースを削除するだけでは AT 機能を停止できないことに注意が必要です。

PL コンフィギュレーション メモリの消去 (応答/ペナルティ)

IPROG は、いずれかの PS プロセッサで動作するアプリケーションが PCAP インターフェイス経由で送信する内部コマンドであり、PL コンフィギュレーション メモリ、すべてのフリップフロップ コンテンツ、およびキー拡張メモリを消去しますが、BBRAM AES キー自体は消去しません。IPROG は、FPGA ファミリの外部 PROGRAM_B ピンのアサートに相当します。このコマンドは、PL コンフィギュレーション メモリ (コンフィギュレーション データ、ブロック RAM、UltraRAM、およびフリップフロップ ステート) を効率的に消去します。

BBRAM のレッド キー ストレージを使用している場合に AES キー消去と IPROG の両方のペナルティが適用されると、既存のイメージ/ビットストリームを復号化できなくなるため、Zynq UltraScale+ デバイスは動作不可能な状態になります。暗号化されたイメージ/ビットストリームでデバイスのセキュア ブートができないということは、不正操作イベントが発生したことを意味します。この時点で、デザインは暗号化されていないイメージ/ビットストリームを読み込むことができ、CT を流出させずに一部の基本機能を利用できます。当然ながら、eFUSE ベースのキーを使用している場合で、enc_only eFUSE がプログラムされている場合は、暗号化されていないイメージ/ビットストリームを読み込むことはできません。

キーの俊敏性 (応答)

キーの俊敏性とは、いずれかの PS プロセッサで動作するアプリケーションを通じて BBRAM の AES 復号化キーを更新または変更する能力を指します (『SBBRAM および eFUSE のプログラミング』(XAPP1319) [参照 10] を参照)。eFUSE ベースのキーは OTP (ワンタイム プログラマブル) であるため、関係ありません。

図 12 は、最初のキーが BBRAM に既にロードされた Zynq UltraScale+ デバイスを示しています。次に外部の暗号化されたイメージ/ビットストリームをロードし、復号化してから、最初の FPGA ロジック デザインを起動して実行できます。

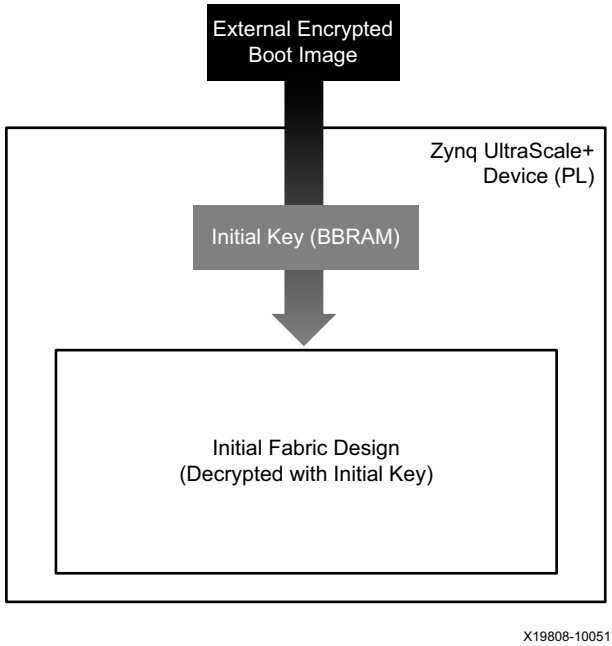

図 12: キーが BBRAM にロードされた Zynq UltraScale+ デバイス

将来的な可能性として、セキュリティ侵害、適切な暗号化の運用、または新規デザインなどによってキー管理イベントが発生し、キーの変更やアップデートが必要になることがあります。何らかのセキュアなキー交換アルゴリズム (PL ロジックで動作する IP コア、または Diffie-Hellman プロトコルなどの PS ロジックで動作するコード) を使用して外部の暗号化キーを取り込むことができます (インターネット経由でも可能)。その後、このキーは PL のロジックまたは PS のコードを使用して復号化され、BBRAM に読み込まれると CRC インテグリティ チェックが内部で実行されます (図 13 を参照)。

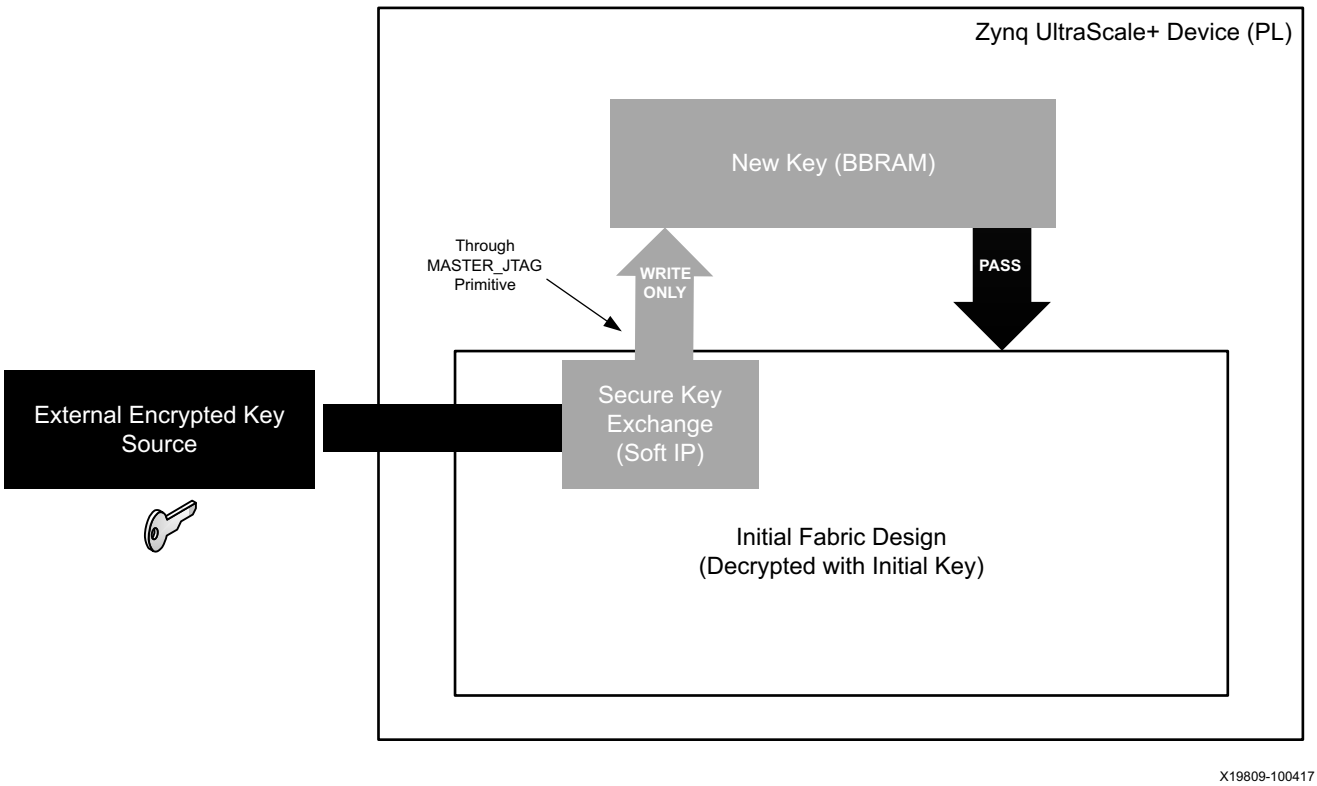

図 13: キー管理イベント

次に、図 14 に示すように POR を実行し、外部の暗号化されたイメージ/ビットストリーム (新しいキーで暗号化) をロードして復号化すると、この新しいキーで復号化された新しい PS および PL デザインを使用できます。

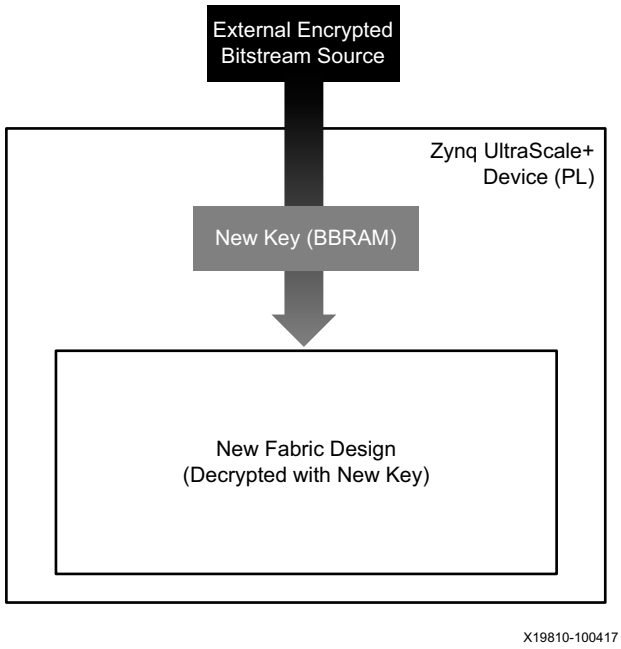

図 14: 新しい PL デザイン

この手法を使用すると、フィールドでキーをアップデートできるため、安全な場所にボードやシステムを移動させる必要がありません。

BBRAM キーのゼロ化 (応答/ペナルティ)

BBRAM レッド キー ストレージを使用する場合、aes_key_clear レジスタ経由で AES キーを消去する際やゼロ化を証明するために aes_status レジスタの検証ビットを読み出す際の適切な条件を決定する PS コードを構築できます。キーがゼロ化されると、同じキーで再プログラムするか、暗号化されていないイメージ/ビットストリームでリブートするまで (機能が制限される可能性がある)、Zynq UltraScale+ デバイスは使用できません。必ず適切な条件でのみ aes_key_clear がアサートされるようにします。多くの場合、このような状態になったフィールドの装置は取り外して中央拠点や製造工場に送り返し、キーをロードして再び有効にする必要があります。

AES キーの消去を IPROG コマンドと組み合わせることで (「PL コンフィギュレーション メモリの消去 (応答/ペナルティ)」を参照)、不正操作イベントに応答して PL コンフィギュレーション メモリを消去することも可能です。

CSU の不正操作の監視と応答 (検出/応答)

表 6 および表 7 では、デバイスが安全に起動した後での CSU の監視機能やオプションの不正操作応答機能について説明しています。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の 「Zynq UltraScale+ MPSoC デバイスのプログラミング ビュー」の章、および『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1087) [参照 8] を参照してください。

表 6: CSU の不正操作監視レジスタ

レジスタ	監視の説明
csu_tamper_12	トランシーバー用の SYSMON 電圧アラーム
csu_tamper_11	PSIO バンク 3 用の SYSMON 電圧アラーム
csu_tamper_10	PSIO バンク 0/1/2 用の SYSMON 電圧アラーム
csu_tamper_9	DDRPHY 用の SYSMON 電圧アラーム

表 6: CSU の不正操作監視レジスタ

レジスタ	監視の説明
csu_tamper_8	VCCPAUX 用の SYSMON 電圧アラーム
csu_tamper_7	VCCPINT_FPD 用の SYSMON 電圧アラーム
csu_tamper_6	VCCPINT_LPD 用の SYSMON 電圧アラーム
csu_tamper_5	APU 用の SYSMON 過剰温度アラーム
csu_tamper_4	LDP 用の SYSMON 過剰温度アラーム
csu_tamper_3	PL SEU エラー
csu_tamper_2	JTAG トグル検出
csu_tamper_1	外部 MIO
csu_tamper_0	CSU レジスタ

不正操作イベント発生後の CSU による応答方法はユーザーが定義できます。表 7 に、各不正操作イベントに対して特定の不正操作応答を得るには、不正操作応答レジスタのどのビットを設定すればよいかを示しています。1 つの不正操作イベントに対して複数の不正操作応答ビットを設定できます。

表 7: 不正操作監視および応答ビット

ビット	応答/ペナルティの説明
4	BBRAM キーの消去 (次の選択肢のいずれかに加える)
3	セキュア ロックダウンして、すべての I/O をトライステートにする
2	セキュア ロックダウン
1	システム リセット
0	システムの割り込み

これらのレジスタは読み出し可能ですが、書き込みアクセス時に 1 回のみ設定できます。つまり、指定した不正操作イベントに対して特定の応答ビットを設定後、その応答を選択しているビットは POR が生じるまでクリアできません。これは、不適切または悪意のあるソフトウェアによって不正操作応答ペナルティが減ることを防ぐためです。不正操作応答はによるペナルティは増えていくのみです。

公開キーの取り消し (応答)

Zynq UltraScale+ デバイスで使用される公開キーは、プライマリ公開キー (PPK) とセカンダリ公開キー (SPK) の 2 種類あります。表 8 に、それぞれの公開キーの特性を示しています。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章および 『Zynq UltraScale+ MPSoC レジスタ リファレンス』(UG1087) [参照 8] を参照してください。

表 8: 公開キーの特性

公開キー	数	場所	取り消し	詳細
プライマリ (PPK)	2	eFUSE 内に外部メモリとハッシュ値	取り消し可能	SPK および認証ヘッダーを認証する目的のみに使用されます。
セカンダリ (SPK)	最大 32	ブート イメージ	取り消し可能	PPK で認証されます。その他すべての認証に使用されます。

不正操作ペナルティのように、現在の PPK/SPK が取り消されると、認証された新しいイメージ/ビットストリームと新しい PPK ハッシュ値または eFUSE にプログラムされた SPK ID を使用してフィールドで安全にアップデートされるまで (または安全な拠点に送り返されるまで)、デバイスは動作不能 (安全に起動できない状態) となります。両方の PPK が取り消された場合、デバイスは基本的に動作できず、起動もできないため再び使用することは不可能です。

不揮発性 (eFUSE) 不正操作イベントのログ機能 (応答)

Zynq UltraScale+ デバイスには 256 ビットのユーザー eFUSE レジスタがあります。このレジスタは、不正操作や管理の記録など不揮発性領域での必要性に柔軟に対応できます。eFUSE レジスタ ビットは、USER_0 から USER_7 の 32 ビット eFUSE レジスタを PS 経由でプログラムします。

重要: これらの eFUSE ビットをプログラムした後、ほかの eFUSE を書き込み不可にプログラムできるため、eFUSE レジスタ ビットがそれ以上プログラムされるのを防止 (「ドアをロック」) できます。これは、misc_user_ctlr eFUSE レジスタの対応するロック ビットをプログラムすることで可能になります。そのため、攻撃者は不正操作ログ情報を上書きできません。

ユーザー アクセス可能な暗号化ブロック (防止)

セキュア ブート後には、ハードウェアに実装された CSU 暗号アクセラレータを利用できるため、それらを PS または PL アプリケーションに使用します。利用できる暗号機能は次のとおりです。

- 機密性: AES-GCM 256 ビット デバイス キーまたはユーザー キー (キー アップデート レジスタ - KUP)。AES-GCM コアは、32 ビット ワード ベースのデータ インターフェイスを備えており、対称キー ベースの暗号化/復号化をサポートします。
- 真正性: RSA-4096 計算用のモンゴメリ乗算器。
- 整合性: 384 ビットのハッシュ計算用の SHA-3/384 エンジン。

これらの暗号アクセラレータを使用するデザインの詳細は、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の付録 「XilSecure Library」、および 『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「セキュリティ」の章を参照してください。

ARM TrustZone (防止)

ARM TrustZone テクノロジをサポートすることによって、同一システム内でのセキュア プロセスと非セキュア プロセスの分離が可能になります (『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] および『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] を参照)。TrustZone テクノロジの基本原理は、すべてのソフトウェアとハードウェアのステートやリソースを信頼できるものと信頼できないものの 2 つの領域に分離することです。

非セキュアな仮想プロセッサは、非セキュアなシステム リソースにのみアクセス可能ですが、セキュアな仮想プロセッサはすべてのリソースにアクセス可能です。リソース アクセスは、AXI バスの AxPROT[1] にマップされている NS フラグを使用してバス アクセスまで拡大されます。システムのあらゆる部分 (デバッグ、ペリフェラル、割り込み、およびメモリを含む) をセキュア ワールドとして設計できます。セキュリティ サブシステムを構築することで、ソフトウェア攻撃や一般的なハードウェア攻撃からアセットを守ることが可能になります。

TrustZone テクノロジの一般的な使用例には、ファームウェアの保護、セキュリティ管理、およびペリフェラル I/O の保護などがあります。

ARM v8 暗号拡張 (防止)

暗号拡張機能は ARM v8 暗号拡張命令をサポートしています。詳細は、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1085) [参照 2] の 「アプリケーション プロセッシング ユニット (APU)」の章を参照してください。この暗号拡張によりアドバンスト SIMD (Single-Instruction Multiple-Data) に A64、A32、T32 命令が新たに追加され、次の処理が高速化しています。

- AES (Advanced Encryption Standard) 暗号化/復号化。
- SHA (Secure-Hash Algorithm) 関数 SHA-1、SHA-224、および SHA-256。
- GCM (Galois/Counter Mode) および楕円曲線暗号などのアルゴリズムで使用される有限体演算。

注記: 暗号拡張は、eFUSE から恒久的に無効化できます。

ザイリンクス メモリ保護ユニット (防止)

ザイリンクス メモリ保護ユニット (XMPU) は、メモリを分割し、メモリおよび FPD スレーブに対して TrustZone 保護を適用します。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「システム保護ユニット」の章、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の 「セキュリティ機能」の章、および『Isolation Methods in Zynq UltraScale+ MPSoCs』(XAPP1320) [参照 20] を参照してください。XMPU は、1 つまたは複数のマスターからのアクセスをプログラム可能なアドレス範囲に限定するように設定できます。

XMPU には次の機能が含まれます。

- スレーブ AXI ポート
- ポイズン出力を備えたマスター AXI ポート
- XMPU をプログラムするための APB スレーブ
- レベルで認識される非同期割り込み出力
- AXI クロック (マスター ポートとスレーブ ポートで共通) および APB クロック
- XMPU にはロック レジスタがあり、これを設定すると POR が生じるまで XMPU にそれ以上のプログラミングを実行できなくなります。

ザイリンクス ペリフェラル保護ユニット (防止)

ザイリンクス ペリフェラル保護ユニット (XPPU) はルックアップ テーブルに基づくペリフェラル保護ユニットです。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の 「システム保護ユニット」の章、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の「 セキュリティ機能」の章、および『Isolation Methods in Zynq UltraScale+ MPSoCs』(XAPP1320) [参照 20] を参照してください。XPPU はペリフェラル、メッセージ バッファー (プロセッサ間割り込みおよび通信用)、およびクワッド SPI フラッシュ メモリを保護します。また、XPPU 自体を保護するメカニズムもあります。

XPPU は XMPU よりも細粒度のアドレス照合を採用しており、非常に多くのアドレス アパーチャを使用して、ペリフェラル、IP インテグレーター、およびクワッド SPI フラッシュ メモリのさまざまな要件を満たします。

XPPU には次の機能が含まれます。

- スレーブ AXI ポート (AxUSER の下位ビットでマスター ID を転送)
- マスター AXI ポート (AxUSER の下位ビットでマスター ID を転送)
- XPPU をプログラムするための APB スレーブ
- レベルで認識される非同期割り込み出力
- AXI クロック (マスター ポートとスレーブ ポートで共通) および APB クロック

AXI/APB 分離ブロック (防止/応答)

ザイリンクスの AXI/APB 分離ブロック (AIB) は、AXI/APB マスターまたはスレーブの電源を切断する前に AXI/APB マスターをスレーブから機能的に切り離す役割を果たすインターコネクトの一部となります。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「インターコネクト」の章および『Isolation Methods in Zynq UltraScale+ MPSoCs』(XAPP1320) [参照 20] を参照してください。AIB は、正しい手順でパワーダウン ステートに移行できるように、分離プロセスの間 AXI および APB インターフェイスを管理します。AIB は、デザイン内の分離を強制する場合にも使用でき、不正操作イベントが発生したときに有効化可能です。

システム メモリ管理ユニット (防止)

システム メモリ管理ユニット (SMMU): 分離サービスを提供します。詳細は、『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085) [参照 2] の「システム保護ユニット」の章、『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137) [参照 3] の 「セキュリティ機能」の章、および 『Isolation Methods in Zynq UltraScale+ MPSoCs』(XAPP1320) [参照 20] を参照してください。SMMU は、I/O デバイスが実際に可能な範囲を超えてアドレス指定できるようにします。メモリを分離しないと、I/O デバイスによってシステム メモリが破壊される可能性があります。SMMU はデバイスを分離して DMA 攻撃を防ぎます。分離とメモリ保護のために、SMMU は DMA 対応 I/O に対するデバイス アクセスを事前に割り当てた物理的アドレス空間のみに制限します。

グローバル トライステート (応答/ペナルティ)

システム デザインによっては、重要なレッド情報が Zynq UltraScale+ デバイス ピンから読み出される可能性があります (暗号化モジュールなど)。不正操作イベントに応答して STARTUP ブロックで GTS 入力がアサートされると、すべての PL 出力が即座にハイ インピーダンス状態になり、デバイス外部へのデータフローが停止します。これは、レッド データのフローを早急に停止するために、IPROG またはキー消去より前に講じる緊急措置です。また、CSU の不正操作レジスタを使用しても、特定の不正操作イベントに応答してセキュア ロックダウンを発生させたり、すべての GPIO をハイ インピーダンス状態にできます。

グローバル リセット (応答/ペナルティ)

ユーザー キー (AES BBRAM ビットストリーム復号化キーではない) などの重要なデータや機密パラメーターは PL ロジック レジスタに格納できます。不正操作イベントに応答して STARTUP ブロックで GSR 入力がアサートされると、すべての PL レジスタ (フリップフロップ) がデフォルト ステートに戻ります。これは、Zynq UltraScale+ デバイス内のすべての機密データを早急に消去するために、キー消去と共に実行される緊急措置です。GSR が、シフト レジスタ ルックアップ テーブル (SRL)、ブロック RAM (BRAM) または UltraRAM (URAM) のコンテンツに影響することはありません。これらはデザインまたは IPROG コマンドで消去する必要があります。

不正操作防止のガイダンス

ここでは、前述したビルトイン シリコン AT 機能と併せて、Zynq UltraScale+ デバイスを使用して不正操作防止デザインを作成するためのガイダンスおよび技術的ヒントを説明します。

デバイス キーの使用制限 (防止)

理想的なセキュリティ対策とはキーの使用を制限することです。最終的には Zynq UltraScale+ デバイスに格納されるキーの使用を最小限に抑える、または使用しないようにすることが目標であり、これによりキーを頻繁に変更する必要性も削減されます。対称キー (AES) の使用を最小限にするには、AES デバイス キーがブート イメージ内のセキュア ヘッダーを復号化するためだけに使用されるようにブート ヘッダーで操作 (OP) キーの使用を指定します。この中には、OP キーとブート イメージの最初のブロック用の初期化ベクター (IV) が含まれています。これにより、最初の FBSL ブロックは OP キーで復号化されます。

また、PPK の非対称キー (RSA) の使用も、SPK の認証にのみ使用されるように最小限に制限する必要があります。PPK キーの使用制限は、ユーザーが安全な場所に格納して確実に保護する必要があるプライマリ秘密キーの露出を抑えることにつながります。

必要な場合にのみ CT を読み込む (防止)

デザインを非クリティカル テクノロジ ブロックとクリティカル テクノロジ ブロックに分割した場合、デザインの非 CT 部分のみを常時に配置し、必要に応じて Zynq UltraScale+ デバイスのパーシャル リコンフィギュレーション (PR) 機能を使用して CT 部分をロードできます。CT の役割が完了したら、PR 領域のブラック ボックス バージョンをロードして CT を消去できます。CT のパーシャル ビットストリームはデバイスの PL 内で任意のアルゴリズムで復号化できます。不正操作イベントが生じた場合には、PR 領域と CT のキー (通常、ブロック RAM または PL に格納される) の両方を消去できます。

例として、図 15 と図 16 に、PL、CPU、および外部メモリ デバイス (PL コンフィギュレーション、PR、CPU コード、および CPU ブート コード用) で構成された一般的なシステムを示します。

図 15 の PR 領域 (「User CT Logic Region」 と表示) は空の状態です。

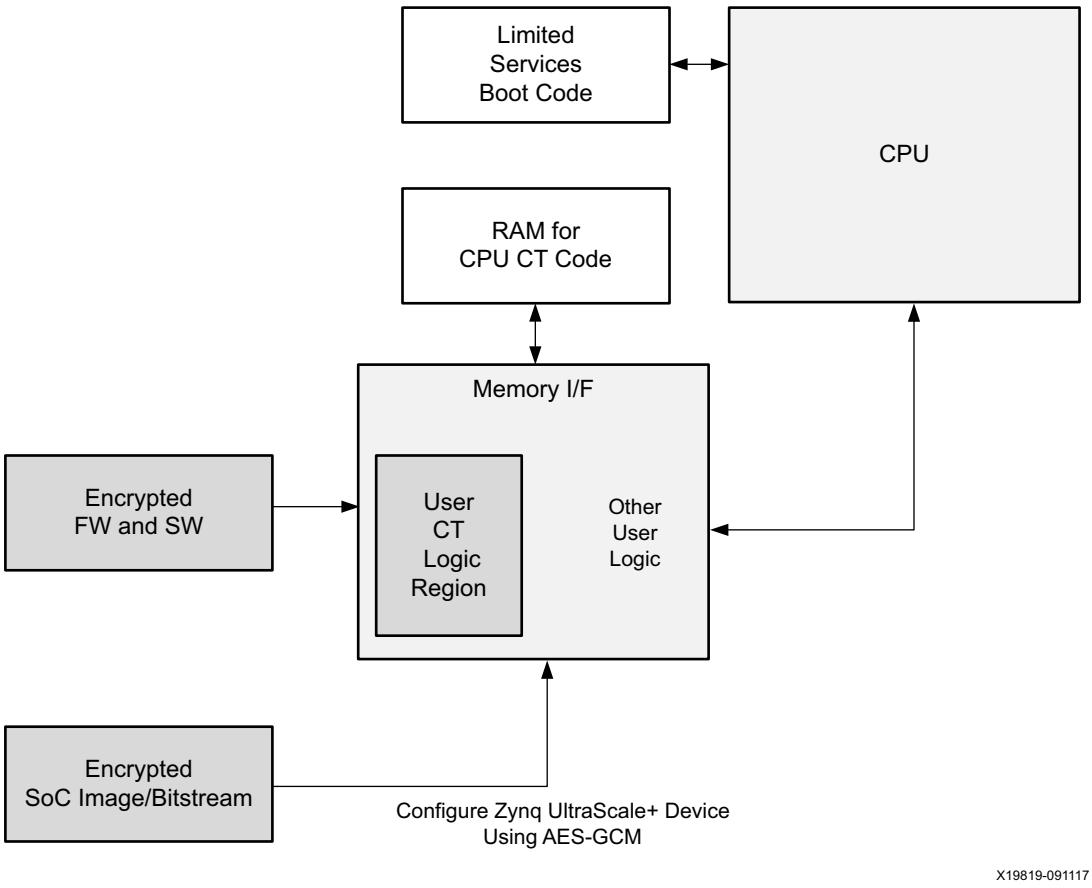

図 15: 使用モデル: システムの CT の保護

図 16 の場合、PR (ユーザー CT ロジック) によって、デバイスの PR 領域に CT ロジックが動的にロードされます。CT の役割が完了するか不正操作イベントが発生すると、PR モジュールの空バージョンをロードすることで、図 15 に示す状態に PR 領域を戻すことができます。

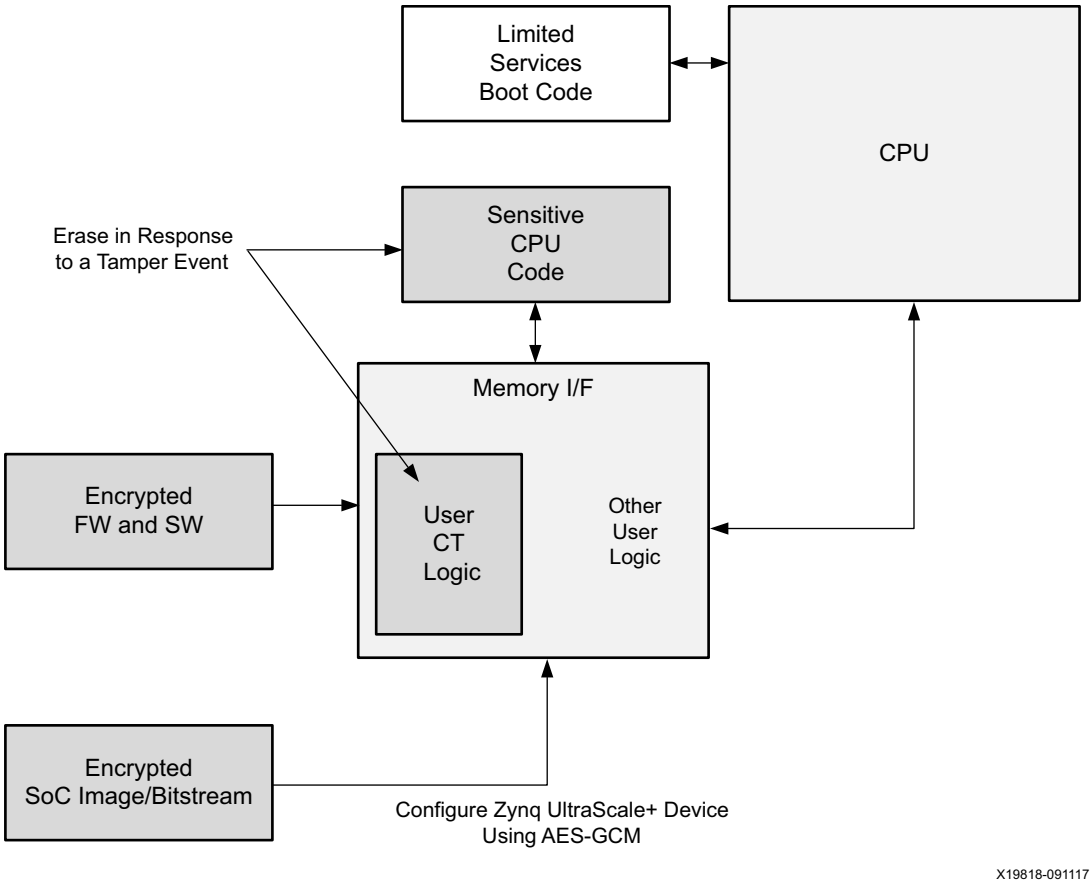

図 16: 使用モデル: システムの CT の保護 - 不正操作へ応答

注記: 不正操作イベントが発生した場合、外部の重要な CPU コード メモリは消去され、暗号化された、消去された、または重要度の低い外部メモリ コンテンツのみが残ります。

これらの例では、PR の実行に PCAP が使用されます。PCAP は信頼できるチャネルであるため、暗号化された PR ビットストリームと暗号化されていない PR ビットストリームのいずれも使用可能です (fg_aes_only eFUSE ビットが設定された eFUSE キーを使用している場合でも可能)。PS または PL にある任意の復号化/認証エンジンで復号化と認証が実行される暗号化かつ認証された PR ビットストリームを常に使用することを推奨しています。

外部シャントによるキーの消去

BBRAM キーを消去する別の方法として、外部シャントを使用して VCC_PSBATT ラインをグランド接続する方法があります。キー消去などの能動的機能はデバイスに電源が投入されてコンフィギュレーションされた後にのみ使用可能なため、Zynq UltraScale+ デバイスの主電源 (VCCINT および VCCAUX) が供給されていない場合には、この方法を用いてキーを消去できます。たとえば、デバイスに主電源が供給される前にシステム レベルの不正操作イベントが検出された場合 (不正操作スイッチがアクティブになるなど)、Zynq UltraScale+ デバイスの VCC_PSBATT ピンへの外部バッテリ電源ラインをオープンにして、何らかのトランジスタ シャントで VCC_PSBATT ピンをグランド接続できます。VCC_PSBATT ピンをグランドにシャントする前にバッテリ接続がオープンになるように回路を設計する必要があります。また、別の方法として、抵抗を介してバッテリを VCC_PSBATT ピンに接続する方法もあります (VCC_PSBATT ピンの最大入力電流 ICC_PSBATT は、バッテリ電圧とリアルタイムクロック (RTC) の有効/無効に応じて、3650 ～ 150nA となる)。詳細は、『ZynqUltraScale+ MPSoC データシート: DC 特性および AC スイッチ特性』(DS925) [参照 19] を参照してください。適切な抵抗値を選択することで、バッテリから過度な電流フローを生じさせることなく VCC_PSBATT ピンをグランドに直接シャントできます。

Zynq UltraScale+ デバイスに電源が投入されていない場合 (VCCINT や VCCAUX などの電圧が存在しない場合、ただし VBATT は例外) で、VCC_PSBATT ピンが適切にグランドにシャントしている場合、BBRAM に格納された AES キーが消去されるまでワースト ケースで最大 200ms かかります。

重要: セキュリティ レベルを高めながら流出を最小限に抑えるには、電圧ができるだけ低いバッテリを使用します。バッテリ電圧レベルの詳細は、『ZynqUltraScale+ MPSoC データシート: DC 特性および AC スイッチ特性』(DS925) [参照 19] を参照してください。

予防策としての BBRAM キーのゼロ化

予防策としてキーのゼロ化を用いる方法があります。イメージ/ビットストリームをロードして復号化した後、システムを配備する前に BBRAM キーを意図的にゼロ化できます。この方法は、発射後のミサイルなど、配備後に電源を切って入れ直す必要のないシステムにのみ有効です。これは eFUSE キーにも使用でき、eFUSE キーの読み出しと書き込みが無効になっていない場合に限り、配備前に PS を介してすべて 1 に書き換えます。

脆弱なキーや重複したキーは使用しない

ユーザー キーにはすべて 0、すべて 1、または反復パターンを使用しないようにします。可能な限り、キーを再利用しないようにします。キーの利用者を厳しく制限する必要があります。つまり、キー値を知る必要がある人のみがキー データにアクセスできるようにします。ランダムなソースを使用してキーを生成することが理想的です。脆弱なキーは使用しないようにします。たとえば、すべて 0 のランダム キーは理論的には可能ですが使用しないでください。Vivado Design Suite で AES-GCM キーを自動的に生成できますが、その場合、現在の日付と時刻に基づいた疑似ランダム プロセスが使用されます。真のランダム プロセスで生成されるキーが最も安全となります。

暗号化システムにおいて、キー管理は非常に重要であり、おそらく最も複雑な要素です。キーに関するその他の役立つ情報は、NIST のキー管理ガイドライン [参照 21] を参照してください。

不正操作ステータス出力をシステムへ送信

不正操作イベントが発生 (ペナルティがアサート) した場合、ユーザー eFUSE 領域にローカルにログを記録する代わり、またはこれに加えてシステムに不正操作ステータス情報を送信することが可能です。今後の監査用に、システムにこの情報を保存できます。IPROG コマンド (不正操作ペナルティ) が実行される前にデータを転送するように設計する必要があります。

Zynq UltraScale+ デバイスのプローブ ポイントへのアクセスを制限

攻撃されにくい FPGA を構築するには、多層アプローチが理想的です。CT を含むすべてのデバイス周囲に堅牢な不正操作バウンダリ (不正操作検出スイッチなど) を使用できます。たとえば、不正操作スイッチがアクティブになった場合に Zynq UltraScale+ デバイスの VCC_PSBATT ラインでシャントをアクティブにできます。プリント回路基板には Zynq UltraScale+ デバイス信号用に埋め込み型のビアと配線を使用し、電源配線を埋め込み層内に配置して (アクセスが困難になる)、適切にデカップリングします (可能な場合は、埋め込みキャパシタンス テクノロジを使用)。JTAG バウンダリス

キャン技術は、ボード レベルのファクトリ テストとして信頼性があります。また量産ボードからテスト ポイントを削除する必要があります。

まとめ

このアプリケーション ノートでは、Zynq UltraScale+ デバイスで現在利用できる AT 機能の概要を説明し、これらの AT 機能を効果的に使用する実際の例を紹介しました。設計初期段階に AT 機能を導入し、そのガイダンスに従うことで、Zynq UltraScale+ デバイスの不正操作防止システム デザインを実現できます。

1 つの AT 機能や手法で常に 100% の効果を挙げたりシステム全体のすべての AT ニーズを満たすことは不可能ですが、攻撃者の作業をできるだけ困難でコストの高いものにしたり、多層アプローチを採用することで、ほとんどの場合に満足できる結果を得ることができます。

FPGA および SoC を含めた新しい集積回路の開発およびテストに使用されるツールとテクノロジは日々進化し、改善されています。同時に、攻撃者が使用するツールも進化と改善を繰り返しているため、最新の AT 機能や手法を把握しておくことが重要です。またザイリンクスは、これらの開発の最先端をリードし、現在および将来においてカスタマー IP を保護するために機能強化と新機能の開発に尽力しています。

Documentation Navigator およびデザイン ハブ

Xilinx® Documentation Navigator (DocNav) では、ザイリンクスの資料、ビデオ、サポート リソースへアクセスでき、特定の情報を取得するためにフィルター機能や検索機能を利用できます。Xilinx Documentation Navigator を開くには、次のいずれかを実行します。

- Vivado® IDE で [Help] → [Documentation and Tutorials] をクリックします。
- Windows で [スタート] → [すべてのプログラム] → [Xilinx Design Tools] → [DocNav] をクリックします。
- Linux のコマンド プロンプトに「`docnav`」と入力します。

ザイリンクス デザイン ハブには、資料やビデオへのリンクがデザイン タスクおよびトピックごとにまとめられており、これらを参照することでキー コンセプトを学び、よくある質問を解決できます。デザイン ハブにアクセスするには、次のいずれかを実行します。

- Xilinx Documentation Navigator で [Design Hubs View] タブをクリックします。
- ザイリンクス ウェブサイトの デザイン ハブ ページを参照します。

注記: Xilinx Documentation Navigator の詳細は、ザイリンクス ウェブサイトの Documentation Navigator ページを参照してください。

参考資料

注記: 日本語版のバージョンは、英語版より古い場合があります。

1. Zynq UltraScale+ MPSoC (ザイリンクスのウェブサイト)
2. 『Zynq UltraScale+ MPSoC テクニカル リファレンス マニュアル』(UG1085: 英語版、日本語版)
3. 『Zynq UltraScale+ MPSoC ソフトウェア開発者向けガイド』(UG1137: 英語版、日本語版)
4. Vivado Design Suite (ザイリンクスのウェブサイト)
5. 『Solving Today's Design Security Concerns』(WP365)
6. 『UltraScale FPGA および UltraScale+ FPGA での不正操作防止デザインの開発』(XAPP1098: 英語版 、日本語版)
7. Security Monitor IP の製品概要
8. 『Zynq UltraScale+ MPSoC Register Reference』(UG1087)
9. 『Zynq UltraScale+ MPSoC PUF Characterization Report』(RPT236)
10. 『SBBRAM および eFUSE のプログラミング』(XAPP1319: 英語版、日本語版)
11. 『Zynq UltraScale+ MPSoC: エンベデッド デザイン チュートリアル』(UG1209: 英語版、日本語版)
12. 「Zynq UltraScale+ MPSoC - ブート時間の見積もり」(ザイリンクス アンサー 67475)
13. Soft Error Mitigation (SEM) コア (ザイリンクスのウェブサイト)
14. 『UltraScale アーキテクチャ ライブラリ ガイド』(UG974: 英語版、日本語版)
15. 『UltraScale アーキテクチャ システム モニター ユーザー ガイド』(UG580: 英語版、日本語版)
16. 『Security Solutions Using Spartan-3 Generation FPGAs』(WP266)
17. Security Requirements for Cryptographic Modules, FIPS PUB 140-2
    www.nist.gov/itl/upload/fips1402.pdf
18. Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, and Claire Whelan.The Sorcerer's Apprentice Guide to Fault Attacks.
    http://eprint.iacr.org/2004/100.pdf
19. 『Zynq UltraScale+ MPSoC データシート: DC 特性および AC スイッチ特性』(DS925: 英語版、日本語版)
20. 『Isolation Methods in Zynq UltraScale+ MPSoCs』(XAPP1320)
21. NIST Key Management Guideline
    csrc.nist.gov/groups/ST/toolkit/key_management.html

改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2017 年 10 月 13 日	1.0	初版

お読みください: 重要な法的通知

本通知に基づいて貴殿または貴社 (本通知の被通知者が個人の場合には「貴殿」、法人その他の団体の場合には「貴社」。以下同じ) に開示される情報 (以下「本情報」といいます) は、ザイリンクスの製品を選択および使用することのためにのみ提供されます。適用される法律が許容する最大限の範囲で、(1) 本情報は「現状有姿」、およびすべて受領者の責任で (with all faults) という状態で提供され、ザイリンクスは、本通知をもって、明示、黙示、法定を問わず (商品性、非侵害、特定目的適合性の保証を含みますがこれらに限られません)、すべての保証および条件を負わない (否認する) ものとします。また、(2) ザイリンクスは、本情報 (貴殿または貴社による本情報の使用を含む) に関係し、起因し、関連する、いかなる種類・性質の損失または損害についても、責任を負わない (契約上、不法行為上 (過失の場合を含む)、その他のいかなる責任の法理によるかを問わない) ものとし、当該損失または損害には、直接、間接、特別、付随的、結果的な損失または損害 (第三者が起こした行為の結果被った、データ、利益、業務上の信用の損失、その他あらゆる種類の損失や損害を含みます) が含まれるものとし、それは、たとえ当該損害や損失が合理的に予見可能であったり、ザイリンクスがそれらの可能性について助言を受けていた場合であったとしても同様です。ザイリンクスは、本情報に含まれるいかなる誤りも訂正する義務を負わず、本情報または製品仕様のアップデートを貴殿または貴社に知らせる義務も負いません。事前の書面による同意のない限り、貴殿または貴社は本情報を再生産、変更、頒布、または公に展示してはなりません。一定の製品は、ザイリンクスの限定的保証の諸条件に従うこととなるので、https://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照してください。IP コアは、ザイリンクスが貴殿または貴社に付与したライセンスに含まれる保証と補助的条件に従うことになります。ザイリンクスの製品は、フェイルセーフとして、または、フェイルセーフの動作を要求するアプリケーションに使用するために、設計されたり意図されたりしていません。そのような重大なアプリケーションにザイリンクスの製品を使用する場合のリスクと責任は、貴殿または貴社が単独で負うものです。https://japan.xilinx.com/legal.htm#tos で見られるザイリンクスの販売条件を参照してください。

自動車用のアプリケーションの免責条項

オートモーティブ製品 (製品番号に「XA」が含まれる) は、ISO 26262 自動車用機能安全規格に従った安全コンセプトまたは余剰性の機能 (「セーフティ設計」) がない限り、エアバッグの展開における使用または車両の制御に影響するアプリケーション (「セーフティ アプリケーション」) における使用は保証されていません。顧客は、製品を組み込むすべてのシステムについて、その使用前または提供前に安全を目的として十分なテストを行うものとします。セーフティ設計なしにセーフティ アプリケーションで製品を使用するリスクはすべて顧客が負い、製品の責任の制限を規定する適用法令および規則にのみ従うものとします。

この資料に関するフィードバックおよびリンクなどの問題につきましては、jpn_trans_feedback@xilinx.com まで、または各ページの右下にある [フィードバック送信] ボタンをクリックすると表示されるフォームからお知らせください。フィードバックは日本語で入力可能です。いただきましたご意見を参考に早急に対応させていただきます。なお、このメール アドレスへのお問い合わせは受け付けておりません。あらかじめご了承ください。