安全なハードウェアシステム開発
ホワイトペーパー

WP100-1.1J, 2021-12-06

著作権について（2021）著作権に関する全ての権利は、Guangdong Gowin Semiconductor Corporation に留保されています。

、Gowin、GOWIN、及びGOWINSEMIは、当社により、中国、米国特許商標庁、及びその他の国において登録されています。商標又はサービスマークとして特定されたその他全ての文字やロゴは、それぞれの権利者に帰属しています。何れの団体及び個人も、当社の書面による許可を得ず、本文書の内容の一部もしくは全部を、いかなる視聴覚的、電子的、機械的、複写、録音等の手段によりもしくは形式により、伝搬又は複製をしてはなりません。

免責事項

当社は、GOWINSEMI Terms and Conditions of Sale（GOWINSEMI取引条件）に規定されている内容を除き、（明示的か又は黙示的かに拘わらず）いかなる保証もせず、また、知的財産権や材料の使用によりあなたのハードウェア、ソフトウェア、データ、又は財産が被った損害についても責任を負いません。本文書における全ての情報は、予備的情報として取り扱われなければなりません。当社は、事前の通知なく、いつでも本文書の内容を変更することができます。本文書を参照する何れの団体及び個人も、最新の文書やエラッタ（不具合情報）については、当社に問い合わせる必要があります。

概要

IoT は、独自のシステム属性を持つさまざまなデバイスを導入しています。2018 年のエリクソン・モビリティレポートによると、2018 年には 10 億のセルラーIoT 接続が行われ、この数字は 2023 年までに 35 億になると予想されています。これらのユニークな IoT ハードウェアシステムのほとんどは、新世代のセキュリティ脅威をもたらしましています。これらの脅威により、攻撃者はデータにアクセスできるだけでなく、公共の環境でデバイスを直接制御および監視することもできるため、個人のセキュリティ、さらにはグローバルセキュリティを危険にさらす恐れがあります。

生産と調達のすべての段階で製品の安全性に抜け穴があります。コンポーネントレベルでは、デバイスは工場でのテスト、パッケージング、または出荷時にセキュリティリスクにさらされます。ボードレベルでは、最終製品の開発、テスト、または製造に脆弱性あります。コネクテッドプロダクトが製造された後、デバイスは、リバースエンジニアリング、ハッキング、および複製の脅威を受けやすくなります。これらすべての状況により、重要なデータがアクセス、監視、または制御される可能性があります。

これらの問題を回避するには、システム内の少なくとも 1 つの集積回路デバイスが RoT（Root of Trust）を確立する必要があります。これらのデバイスは、システムの暗号化機能を提供します。これは、セキュアブート、ファームウェアの認証、キー, 証明書, 署名の生成または検証、およびデータの暗号化または復号化に使用できます。

RoT デバイスは、信頼チェーン(Chain of Trust)を通じてシステムの残りの部分に安全機能を提供します。RoT デバイスが侵害されると、システム全体が脅かされます。この点から見ると、これはシステムで最も重要なデバイスです。したがって、チップの製造から最終製品まで、RoT デバイスの機能を完全に確保することが重要です。

暗号化関数は、キーペアを使用してシステム機能を識別および確認します。IoT デバイスを製造する半導体メーカーは、IoT デバイス内の秘密キーとマッチングするルートキーを確立できる必要があります。秘密キーはアクセス不能であり、デバイスから離れることはできません。デバイスの製造中に秘密キーにアクセスできる場合、デバイスが複製または攻撃される可能性があります。さらに、秘密キーがデバイスの Flash またはコンフィギュレーション情報（fuse）に保存されている場合、キーはチップ製造プロセス中に漏洩するか、リバースエンジニアリングされる可能性があり

ます。

この 2 つの問題を解決するために、RoT デバイスには SRAM PUF（Physical Unclonable Function：物理的な複製防止機能）が必要であり、PUF はシリコンの固有のプロパティをランダムな識別子として使用します。この識別子は、リバースエンジニアリングされる可能性のある特定の領域に保存するのではなく、デバイスの電源投入時にキーペアを生成するために使用されます。さらに、複製を防ぐために、工場からの RoT デバイスの証明書が必要になります。この証明書には、暗号化エンジンのルートキーペアに基づく署名があります。デバイスメーカーの承認の署名により、デバイスの信頼性を検証し、RoT デバイス自体がクローンではないことを確認できます。

RoT デバイスのセキュリティ要素がシステムの他の部分と互換性があることを保証するには、標準への準拠も重要です。従って、米国国立標準技術研究所によって設定された、乱数生成の SP 800-90 とプラットフォーム・ファームウェア・レジリエンス(PFR)の SP 800 193 など標準への準拠は、セキュリティと互換性の両方にとって重要な要素です。

安全デバイスと RoT デバイスの選択

従来、特定のシステムの安全デバイスには、MCU と FPGA の 2 つのオプションがありました。いずれのシステムにも、それぞれ独自の長所と短所があります。MCU は、ライブラリおよび API の承認を簡単に取得できるため、使いやすいです。また、これらのライブラリおよび API はデバイス間での移植も簡単です。たとえば、FreeRTOS および MBED TLS は組み込み IoT システムで広く使用されており、このシステムで TCP/IP および TLS/SSL を簡単に取得できます。MCU の 1 つの欠点は、IO 数の不足による、システムのセキュリティ機能に必要なインターフェースの数が足りないことです。もう 1 つの欠点は、MCU が実行時に自身のブートメモリを検出できないことです。

FPGA には、多数の IO、低遅延、およびシステムコンポーネントの並行チェックという利点があります。多数の IO により、システム内のより多くのコンポーネントを制御および監視でき、低遅延により、システムコンポーネントをより高速にチェックでき、並列コンピューティングによりシステム全体をより高速にチェックできます。ただし、その主な欠点は、MCU ほど使いやすいわけではないことです。たとえば、プロセッサと大量のメモリがない場合、FPGA は TCP/IP と SSL スタックを有効にすることは非常に難しく、OEM の難易度も高くなります。

したがって、MCU および FPGA ファブリックを備えたデバイスに安全機能を低コストおよび低消費電力で統合することは望ましいです。同時に、エッジデバイスからサーバーまでの幅広いアプリケーションに対応するパッケージが必要です。これにより、より良いオプションが提供され、必要に応じてシステムが最適化されます。FPGA ファブリックは、高速のパワーオンおよび並列検出を実現できるほか、MCU の使いやすさとライブラリ統合は、開発時間を短縮できます。

Gowin SecureFPGA™ -エッジ、IoT、サーバーシステム向けのセキュア µSoC FPGA

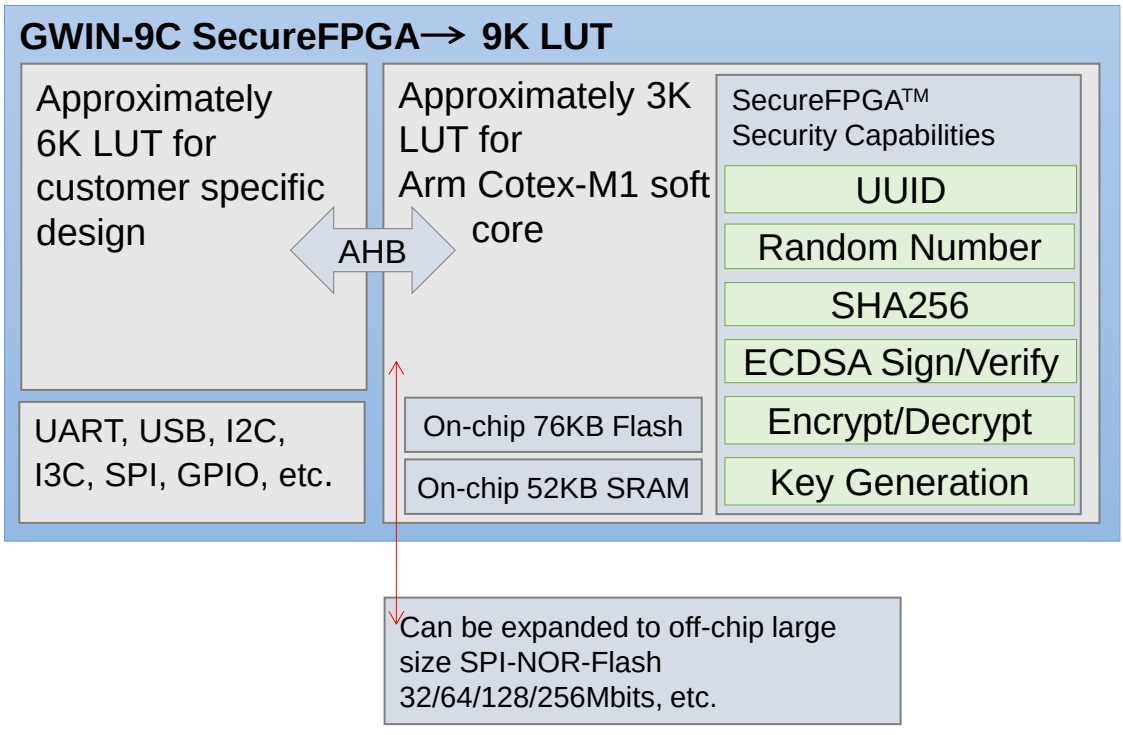
RoT デバイスセキュリティにおける最新の技術革新である Gowin の SecureFPGA™は、MCU と FPGA の利点と、エッジ、IoT、およびサーバアプリケーションに必要なセキュリティ機能とを兼ね備えています。SecureFPGA は、工場フロアから最終製品の毎日の使用までの攻撃を防ぐために設計された Gowin ジェニュインデバイス認証を備えた SRAM PUF テクノロジベースのセキュリティライブラリを提供しています。

このデバイスは、IoT およびサーバーアプリケーションのニーズに対応できる BGA、QFN、および TQFP の幅広いパッケージをサポートします。さまざまな IoT パッケージがあります。サーバー向けパッケージは、アプリケーションに応じて QFN、BGA、TQFP が選択できます。

フル機能のセキュリティライブラリ

Gowin SecureFPGA™ は、SRAM PUF テクノロジーと ECC（Elliptic Curve Cryptography：楕円曲線暗号化）に基づいたセキュアコンポーネントと、フル機能のセキュリティライブラリを提供することで、現在のセキュリティの問題を解決しようとしています。さらに、Gowin は Intrinsic ID と提携して BroadKey-Pro セキュリティライブラリを提供しています。開発者は、暗号化ツールを使用して Gowin SecureFPGA デバイスのアプリケーションの RoT を作成したり、実績のある成熟したセキュリティソリューションを使用してマルチデバイス・システムの RoT を提供したりできます。

Figure 1 GW1N-9C SecureFPGA™ Device



Gowin SecureFPGA™ のセキュリティ機能

- ビットストリームロック - デバイスのビットストリームのオフチップ読み出し可能性を排除します。
- 工場プロビジョニング - コード、UUID、CSR、および証明書をアクティブ化します。
- 内部デュアルブート Flash - ファームウェア署名チェックによるオンラインおよびリモートアップグレードが可能です。
- SRAM PUF - 電源投入時にルートデバイスのキーを生成し、Flash には保存しません。
- UUID - SRAM PUF ルートキーペアで署名された一意のデバイス識別子。
- デバイス証明書 - デバイスを SRAM PUF ルートキーペアで署名された本物の Gowin デバイスとして検証します。
- ECDH 暗号化/復号化 - ECC キーペアコードに基づいた AES128/192/256 エンジン。SRAM PUF テクノロジーに基づきます（一意またはランダム）。
- 非対称キーペアの生成 - SRAM PUF テクノロジーに基づきます（一意またはランダム）。
- ECDH 対称キーの生成 - SRAM PUF テクノロジーに基づきます（一意またはランダム）。
- ECDSA 署名 - 生成と検証。
- 乱数ジェネレータ - SRAM PUF および AES に基づきます。

セキュリティソリューションの成熟度、コンプライアンス、および証明書

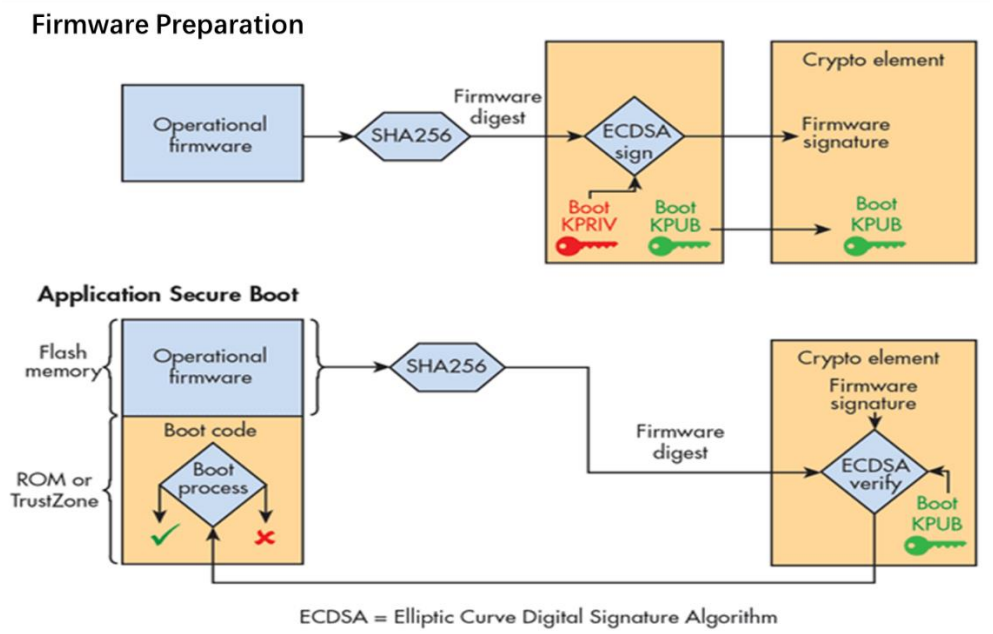
Gowin は Intrinsic ID と提携して、Gowin SecureFPGA デバイス内に BroadKey-Pro セキュリティライブラリを提供しています。Intrinsic ID は、業界で最も成熟した SRAM PUF テクノロジーソリューションの 1 つを提供し、多くの半導体メーカーに採用されています。数年前から業界で認められており、最近、2019 IoT Breakthrough Awards で「IoT Security Product of the Year」に選ばれました。FIPS 140-2 付録 B と中国の OSCCA 規格に準拠し、1 億 2500 万を超える IoT デバイスに使用されています。最後に、Intrinsic ID のセキュリティソリューションは、RoT デバイスに高水準のセキュリティ保護を提供しながら、さまざまな分野で広く使用されています。証明書には、EMVCo、Visa、CC EAL6 +が含まれます。

典型的なアプリケーション

セキュアブートとセキュアソフトウェアの更新

セキュアブートは、ハッシュ処理し、キーを使用して署名を生成し、以前に作成した署名と照合して検証するプロセスです。これにより、デバイスは、ファームウェアを実行する前に、ファームウェアが改ざんされていないかどうかを確認できます。

図 2 セキュアブート



組み込みアプリケーションの場合、セキュアブートは、最初にキーペアの秘密キーを使用してファームウェアで署名を生成します。この署名は、実行時の比較のためにデバイスに保存されます。署名が生成されて保存されると、少数のブートコードが公開キーを使用して署名を生成し、事前に生成されてデバイスに保存された署名と照合します。

図 3 SecureFPGA™ - セキュアブートの準備

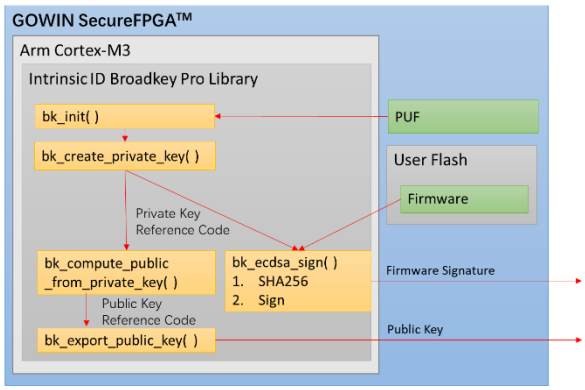
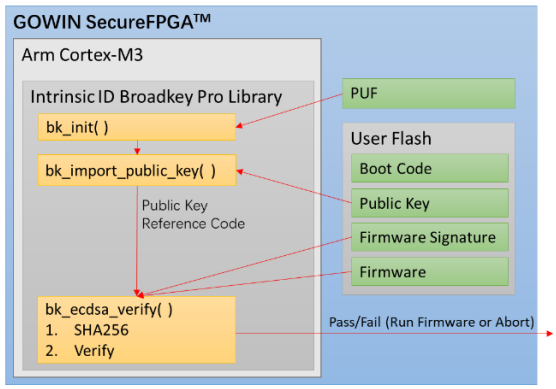
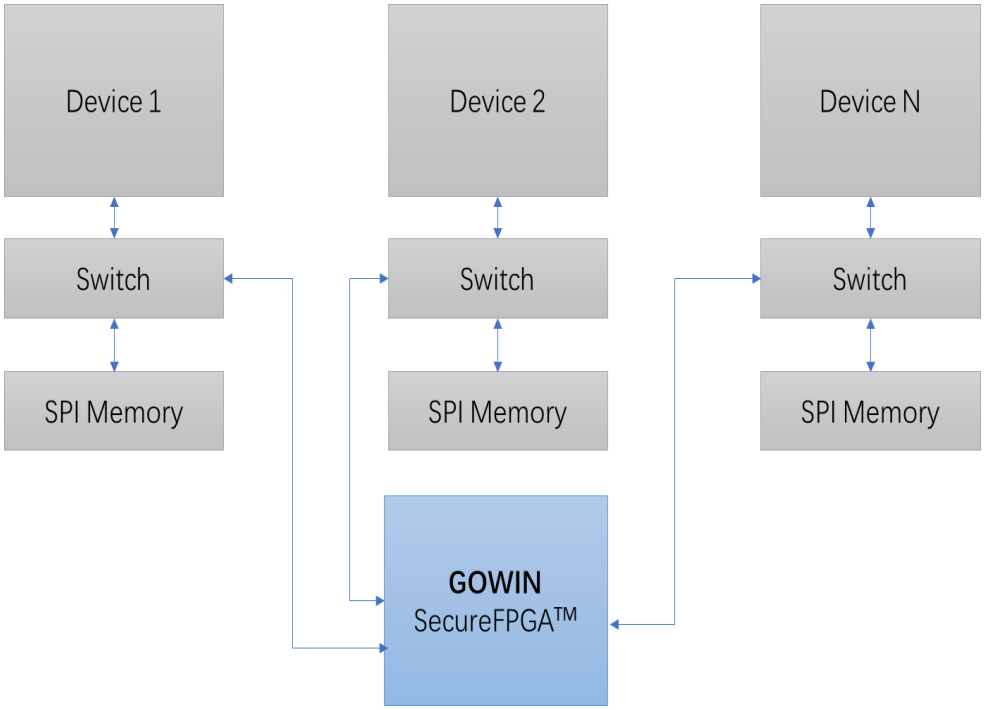


図 4 SecureFPGA™ - セキュアブートの検証



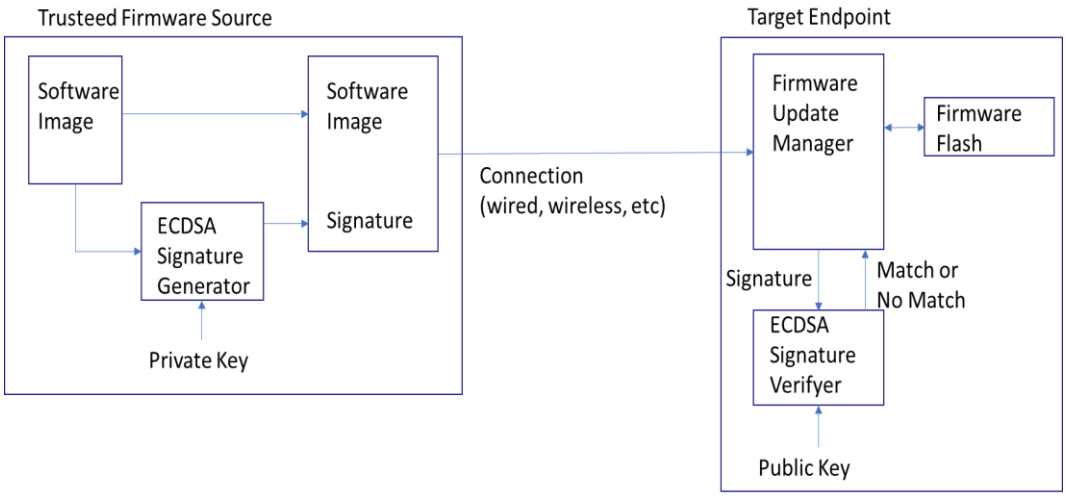
これは、サーバー上の複数のデバイスのファームウェアの検証にも当てはまります。各ファームウェアには、秘密キーによって生成された署名があります。次に、電源投入時に、Gowin SecureFPGA 製品は各デバイスのファームウェアの署名を検証します。

図 5 サーバーアプリケーションでのセキュアボート



デバイスのセキュアブートとサーバーアプリケーションでのセキュアブートに加えて、セキュアファームウェアの更新も可能です。この場合、ファームウェアはソースプログラムによって署名され、何らかの媒体（Webやケーブルなど）を介してデバイスに送信されます。デバイスは、ファームウェアを更新する前に公開キーを使用して検証するか、その基本イメージの使用を保持できます。

図 6 セキュアファームウェアの更新



データの暗号化

データの暗号化を必要とするアプリケーションは多くあります。たとえば、デバイスは Flash または RAM 内のデータまたはファームウェアを個別に暗号化または復号化できるため、プレーンテキストは保存されません。または、あるデバイスが暗号化または復号化されたデータを交換キーを持つ別のデバイスと交換し、これらのデータが送信中に漏洩しません。

図 7 内部デバイスの暗号化/復号化フロー

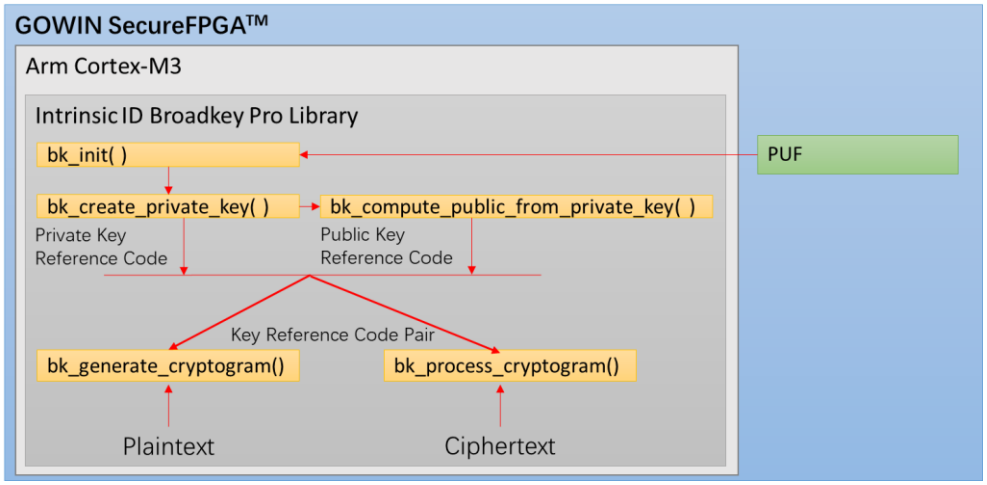
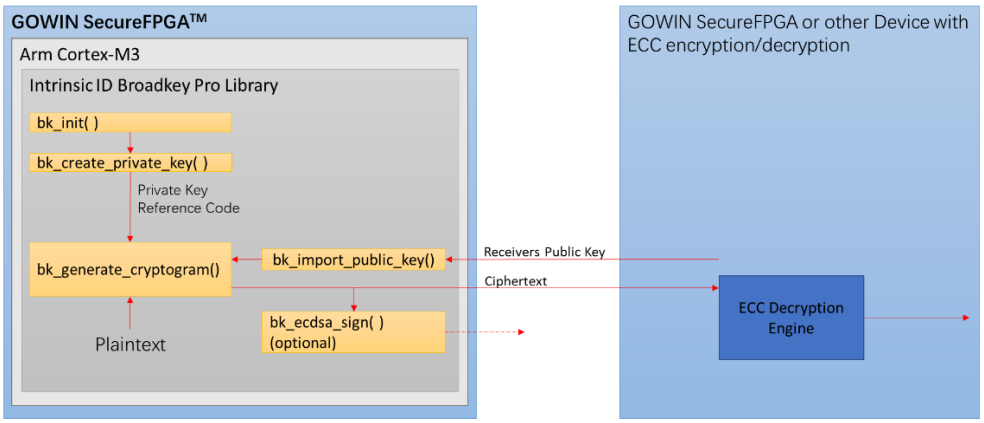


図 8 デバイス間の暗号化/復号化フロー



製造

製造プロセス全体のセキュリティを確保するために、Gowin は特別な SecureFPGA デバイスを提供します。SecureFPGA は、テスト中にアクティベーションコードを提供します。これにより、デバイスは常に同じルートキーペアを生成できます。SRAM PUF エンジンで生成されたルート秘密キーは、ユーザーやデバイスの外部に公開されることはありません。デバイス内のセキュリティ機能を果たす場合にのみ使用でき、「キーコード」を介してユーザーが呼び出すことができます。コンフィギュレーション中に、ルート公開キーがデバイスからエクスポートされます。証明書署名要求（CSR）または UUID が形成されます。これは、サードパーティによって認証できます。または、Gowin が証明書承認（CA）サービスを提供して、工場内の各デバイスの証明書を生成します。Gowin の CA サービスは、デバイスの一意の証明書を検証することによりデバイスが本物であることを確認します。本物でない場合は否認します（詳細については Gowin の技術サポートにお問い合わせください）。これらの機能により、デバイスが一意の識別情報を持つ本物の製品であり、製造から最終製品ライフサイクルまでデータが漏洩する恐れのある Flash にデータを保存しないことが確保されます。

結論

Gowin SecureFPGA 製品は SRAM PUF 技術ベースの信頼のルート（Root of Trust）を提供します。これらのデバイスを複製、クローン、予測することは事実上不可能です。これにより、secure key の生成と保存、デバイス認証、柔軟な key の提供、チップ資産管理などのアプリケーションに非常に適しています。各デバイスには、デバイスの外部または開発や製造中に暴露されることのない一意のキーペアがあります。Intrinsic ID BroadKey-Pro セキュリティライブラリは Gowin SecureFPGA デバイスに付属しており、一般的なセキュリティ機能をユーザーアプリケーションに簡単に統合できます。GOWIN SecureFPGA は、コンシューマ、インダストリアルル IoT、エッジ、およびサーバー管理などの広範な分野に使用できます。

関連資料

1. Columbus, Louis.“2018 Roundup Of Internet Of Things Forecasts And Market Estimates.”Forbes, Forbes Magazine, 18 Dec. 2018, www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#4b33a2747d83.
2. Lazich, Milan.“Intrinsic ID's BroadKey Named 'IoT Security Product of the Year' in 20.”PRWeb, 3 Jan. 2019, www.prweb.com/releases/intrinsic_ids_BroadKey_named_iot_security_product_of_the_year_in_2019_iot_breakthrough_awards/prweb16012275.htm.

テクニカル・サポート

GOWIN セミコンダクターは、包括的な技術サポートをご提供しています。使用に関するご質問、ご意見については、直接弊社までお問い合わせください。

Web サイト: www.gowinsemi.com/ja

E-mail: support@gowinsemi.com

GOWIN
PROGRAMMING FOR THE FUTURE