STM32L4 – デバイス電子署名

Revision 1

life.augmented

Dec- 2015

STM32のデバイス電子署名のプレゼンテーションへようこそ。

本プレゼンテーションでは、デバイスIDやシリアルナンバー等で
使用されるデバイス電子署名について説明します。

概要

- デバイス電子署名はアプリケーションで読み出し可能なデバイスIDを提供します
  - 96ビットのユニークID
  - フラッシュサイズ、パッケージタイプの情報

アプリケーションの利点

- 暗号鍵、および、シリアル番号
- ソフトウェアのライセンス – ソフトウェア・ハウスは納品後のファームウェアに対して特定のUID範囲の制限をかける事ができます
- 複数プラットフォーム・ファームウェアにおいてアプリケーションはパッケージタイプとメモリサイズを特定できます

life.augmented

デバイス電子署名は、ダイの情報、ユニークデバイスID（UID）、メモリサイズやパッケージタイプ、較正情報などのデバイスのほかの情報を含むレジスタセットを提供します。

アプリケーションでは、ユニークIDを使用して暗号鍵の一部を担ったり、シリアル番号やソフトウェア納品後のライセンス管理等にUIDを使用することが可能です。

主な特長

工場出荷時に書き込み済み

- UID はSTの工場で書き込み済み
  - ユーザによる変更はできません
- デバイス情報データ
  - フラッシュサイズ
  - パッケージタイプ

アプリケーションの利点

- セキュリティ、および、シリアル化などに使用可能なデバイスのユニークID
- 複数プラットフォームファームウェアのためのデバイス設定情報
- 読み出し専用情報
- 利用が容易

life.augmented

ユニークID、および、他の情報がSTの工場で書き込み済みで、ユーザが変更することはできません。
このIDは、暗号鍵やシリアル番号、または、ソフトウェアライセンス等に使用することができます。
これらのレジスタに格納された情報をユーザが変更することはできません。

ユニークデバイスIDレジスタ

4

読み出し専用ユニークデバイスID

- ユニークデバイスIDは96ビットのレジスタで以下で構成されています
  - ウェハーのXとYの座標
  - ロットとウェハー番号
- ユニークデバイスIDは各パーツで固有のIDです
- ユニークデバイスIDの全てのビットが使用されるわけではありません
  - レジスタに書き込まれているデータの範囲には制限があります（例　XおよびY座標）
    特定のレジスタ幅よりも小さい
    - 要求により特定のデバイスで0にて固定されていない有効ビットの情報を抽出すことも可能です
  - あるデバイスではレジスタの幾つかのビットは常に0です
  - セキュリティ関係のアプリケーションでは、暗号鍵を生成する際UIDの一部のみを使用することがあります

life.augmented

ユニークデバイスIDは96ビットのレジスタで、ウェハー上のダイの座標、ロット番号、および、ウェハー番号から生成されています。
レジスタの幾つかのビットはこれらの記録を格納する為に予約済みとなっています。
このIDはSTにより製造された各パーツにおいて固有です。
ユニークID内の各記録には、XおよびY座標などのように範囲があるため、デバイスID内の全てのビットが使用されているわけではありません。
これは、使用ビット数が重要なパラメータとなるセキュリティ用途では注意するべき点です。
このようなアプリケーションでは、デバイスIDの一部のみを使用し、固定ビットを使用するのを避けることがあります。

参考資料

- 詳細は以下の資料をご参照下さい
  - リファレンス・マニュアル（STM32L4x6の場合、RM0351）

詳細情報に関しては、主にデバイスのリファレンス・マニュアルとデータシートをご参照下さい。