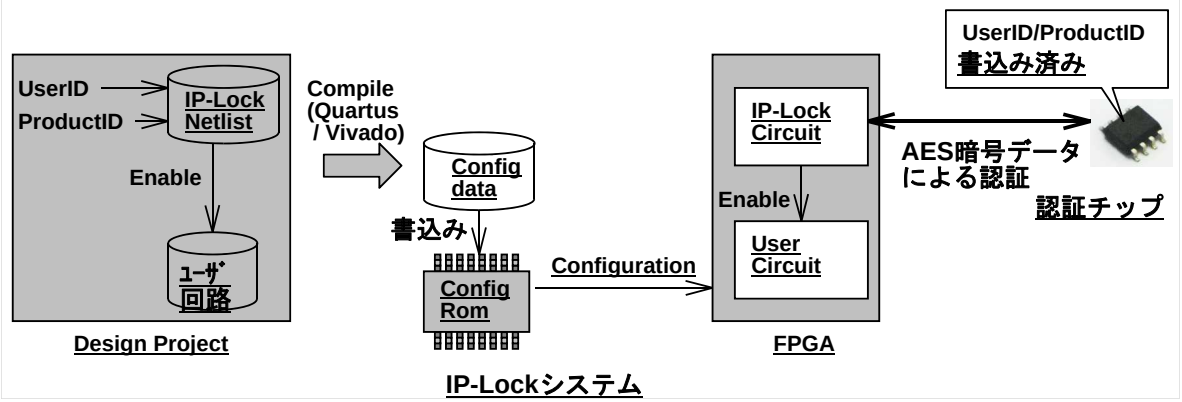
FPGAデータを不正な複製からプロテクト

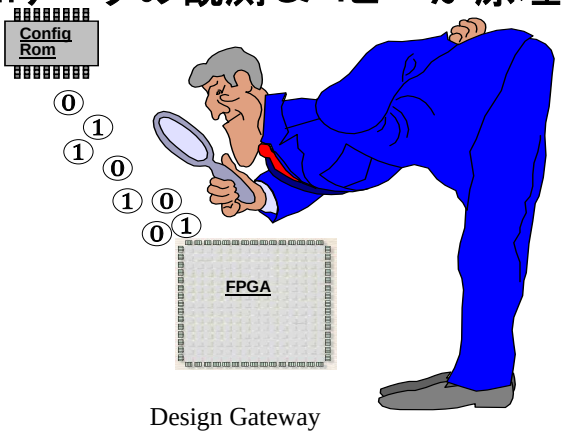
IP Lockとは

- FPGA回路データのセキュリティ・システム
- 認証チップを外付けしFPGAのIOピン経由で通信
- ユーザ回路と暗号処理ロジックを結合しコンパイル
- 暗号処理ロジックが認証チップを検出



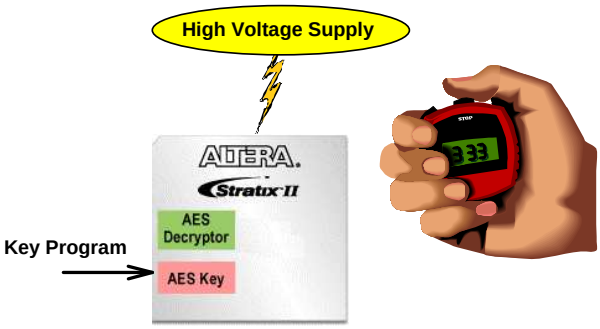
IP Lock開発の背景

- IP保護の重要性
  - FPGA規模に比例し製品開発コスト・期間が著しく増加
  - 回路データをコピーされることによる被害損失は甚大
- FPGAはコンフィグ・データが外部観測可能
  - ConfigRomデータの観測＆コピーが原理上防げない



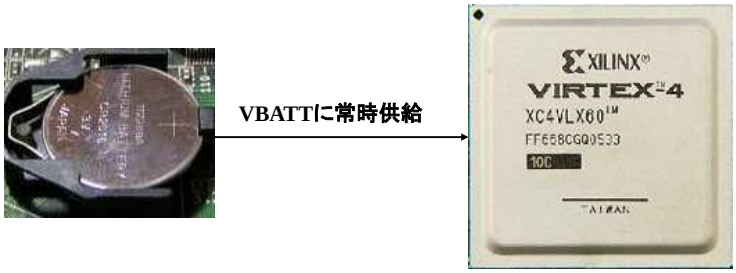
従来のIP保護手法(I社の場合)

- I社の保護方法
  - Device内部の不揮発領域にAESキーを書き込む
- デメリット
  - 書き込み用の特殊な高圧電源がユーザ基板上で必要
  - 電源印加時間に制限(超過するとダメージの恐れ)



従来のIP保護手法(X社の場合)

- X社の保護方法
  - AESキーを内部SRAMメモリに記憶
- デメリット
  - VBATT常時供給用として外部電池が必要
  - 製品寿命が電池寿命に依存してしまう



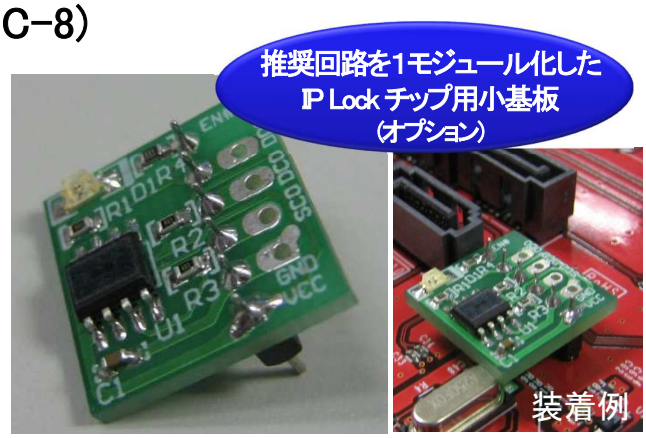
IP Lockのメリット

- 暗号Configがサポートされないデバイスでも適用可
  - 暗号Configデバイスでもセキュリティレベルが更に向上

- 特殊な電源が不要(1.8/2.5/3.3V単一電源で動作)
  - 既存の電源回路そのままで追加電源の必要なし
- ランダムシードの常時更新により耐性を強化
  - 信号発生エミュレーションからプロテクト

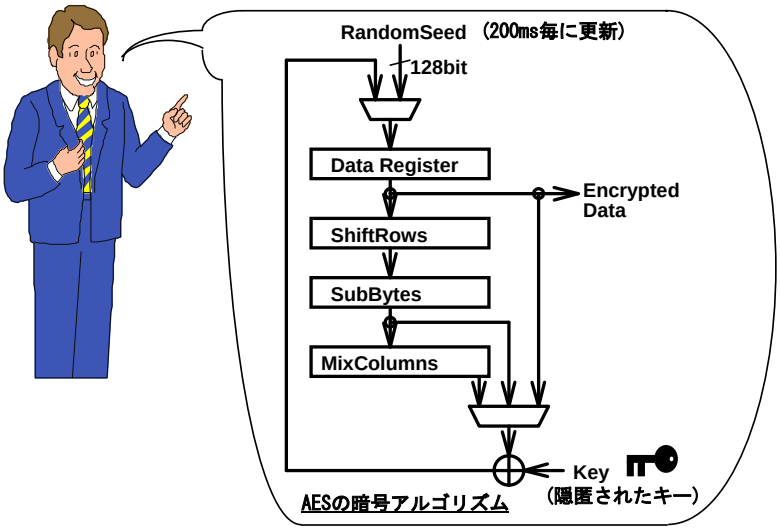
IP Lockのメリット(続き)

- ProductIDの設定で認証チップ移植から保護
  - 製品毎にセキュリティ機能を用意
- 実装が容易
  - FPGAの汎用I/Oピンを2Pin分のみ使用
  - 小型パッケージ(SOIC-8)



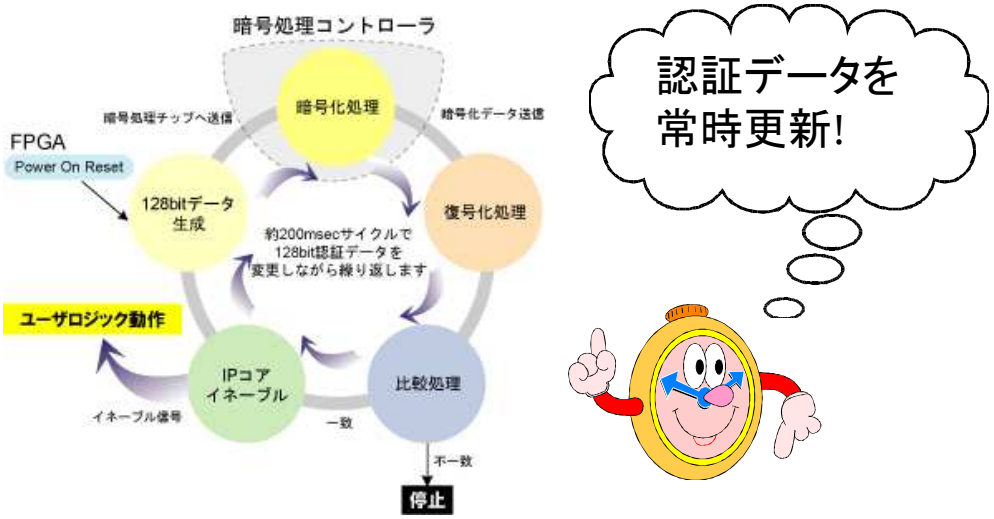
IP Lockの技術1:AES暗号化

- 128bit-AESによる実証済みの暗号強度
  - アルゴリズムは一般公開済み
  - キー値のみで暗号を保持



IP Lockの技術2:リアルタイム認証

- 約200ms毎に認証データを変更
  - PowerUp時の一度のみではなく常時継続した認証
  - 外部認証チップ不在を検出すると即時コア・ロック



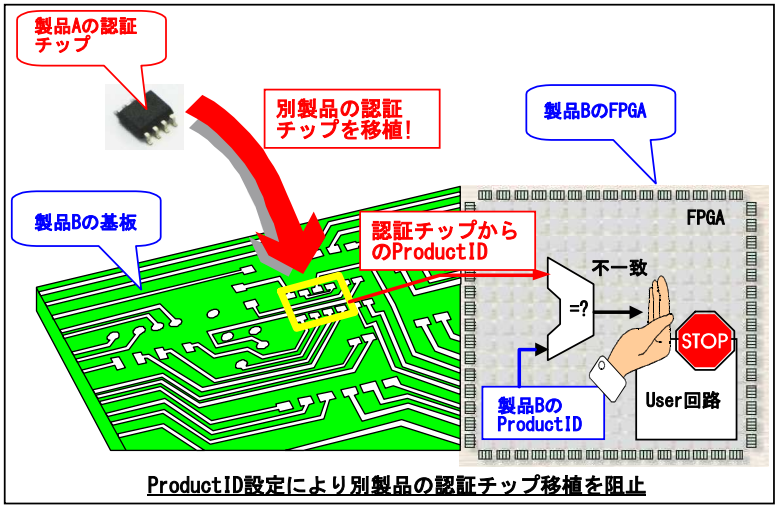
IP Lockの技術3:RNG

- 自然現象を応用した完全ランダムシード発生機能
  - 解読に対して非常に強固な耐性を発揮

IPLock実機のRNG発生データ評価結果例

IP Lockの技術4：ProductID

- 製品別にProductID設定が可能
  - 32bitのProductIDが一致しないと開錠せず
  - 別製品の認証チップ移植からプロテクト



ProductID設定により別製品の認証チップ移植を阻止

サポートデバイスと必要リソース

- Intel向けIP Lock

  - 5シリーズおよび最新10シリーズ・デバイスをサポート(*)
  - 使用セル数：約1280LE
  - 使用メモリ数：24,576メモリ・ビット
- Xilinx向けIP Lock

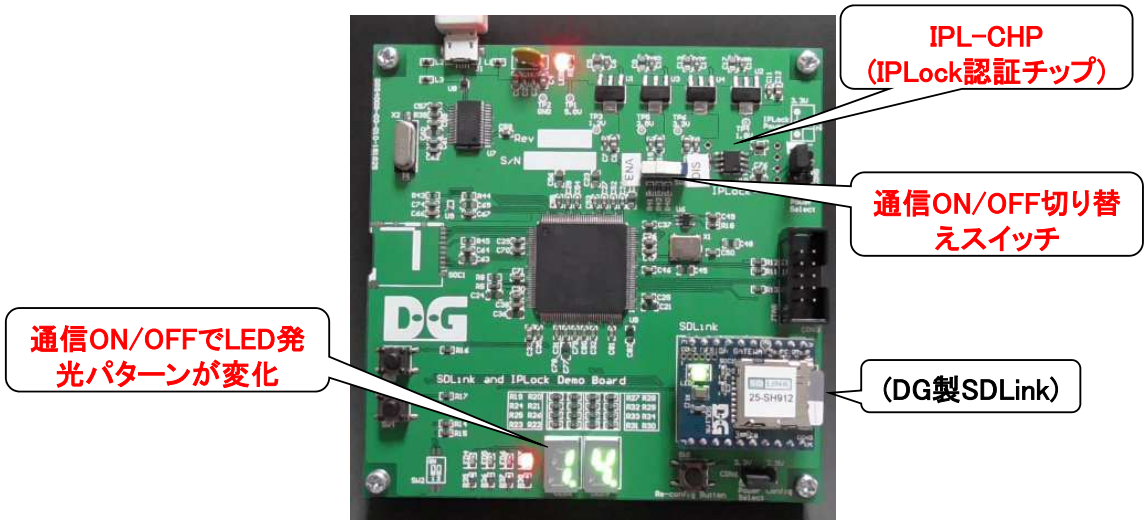
  - 7シリーズおよび最新UltraScale(+)をサポート(*)
  - 使用スライス数：約350Slice
  - 使用メモリ数：2ブロックRAM

(*) サポートデバイスの最新情報についてはサポート・リストをご確認ください

URL : https://dgway.com/products/IPLock/IPL-LIST.pdf

評価ボード

- IP Lock評価ボード（弊社製SDLink評価兼用ボード）
  - 通信のON/OFFでリアルタイム認証機能の確認



IPLock評価ボード（SDLink評価兼用）

製品ラインナップ（認証チップ）

- 低電圧対応版
  - 製品名：IPL-CHP1.8V
  - 動作電圧：1.8V, 2.5V, 3.3Vで動作
  - 1.8V I/Oを必要とする場合に最適

- 従来版
  - 製品名：IPL-CHP
  - 動作電圧：2.5V, 3.3Vで動作
  - 低電圧対応版より安価

製品ラインナップ(パッケージ)

- 試作向けパッケージ (ラボラトリーズ・パック)
  - 各パックごとに固有のProductIDが認証チップに書き込み済みのため、少量使用に最適
  - 認証チップ10個パックセット/30個パックセットを用意
    - 型番:IPL-010L (10個パック) / IPL-030L (30個パック)

- 量産向けパッケージ
  - IP Lockライタ(IPL-003WR)とブランクチップ(IPL-CHP/IPL-CHP1.8V)
  - IP Lockライタから任意のProductIDをブランクチップに書込むことが可能なため、製品別にIDを指定したい場合に最適

IP Lockライタ IPL-003WR

結論:ユーザにとっての利点

- 貴重な回路データ資産を確実に保護
  - 128bit-AESにより実証されたセキュリティ強度
  - 常時認証により信号発生エミュレーションから保護
- 使いやすさで効率アップ
  - セキュリティ機能のないFPGAにも適用可能
  - 特殊な外部電源が不要
  - 最小限の基板占有面積(SOIC-8で2信号の通信)

問い合わせ

- ホームページに詳細な技術資料を用意
  - http://www.dgway.com/IPLock.html
- 問い合わせ先
  - 株式会社Design Gateway
  - E-mail : info@dgway.com
  - FAX : 050-3588-7915
  - URL: http://www.dgway.com

改版履歴

Rev.	日時	履歴
1.0J	2010/7/15	初期版作成
1.2J	2013/11/6	IPLock小基板の記載を追加
1.3J	2019/5/28	低電圧対応版(IPL-CHP1.8V)の記載を追加