



MAXIM

1-Wire®チュートリアル

FPGAセキュリティ

大きな成長が期待されるFPGAの売上げ

- 世界のFPGA市場は2010年に67億ドルまで伸びると予測されています。
 - » Gartner Research (2006)
- 低コストFPGAは成長が期待される主要部品です。主要マーケットは民生、オートモティブで、DSPやマイコンを置き換えていくでしょう。
- 低コストFPGAの売上げは、2010年に全FPGAの売上げの25%になるでしょう
=17.5億ドル
 - » iSupply (2006)



1-WireメモリによるFPGAセキュリティ

— 課題

- オリジナルの設計と契約製造サービスが米国以外で年率15%で成長し続けている。
 - » Global Trends (2006)
- ビットストリーム/設計がコピー/クローンにさらされる恐れがある。
- 低コストFPGAファミリには暗号化機能が内蔵されていない。
- ユーザ指定のFPGA設定コードが外部メモリにある。

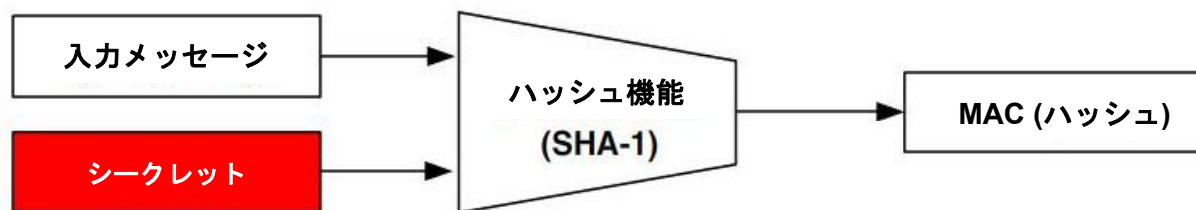
— ソリューション

- 1-Wireセキュアハッシュアルゴリズム(SHA-1)メモリソリューションを使ってFPGA設計の安全性を確保

1-WireメモリによるFPGAセキュリティ

– SHA-1 (Secure Hash Algorithm)とは？

- 入力メッセージとシークレットを使ってメッセージ認証コード(MAC)を計算するパブリックハッシュ機能
- 特性: 非可逆、衝突耐性、アバランシェ効果



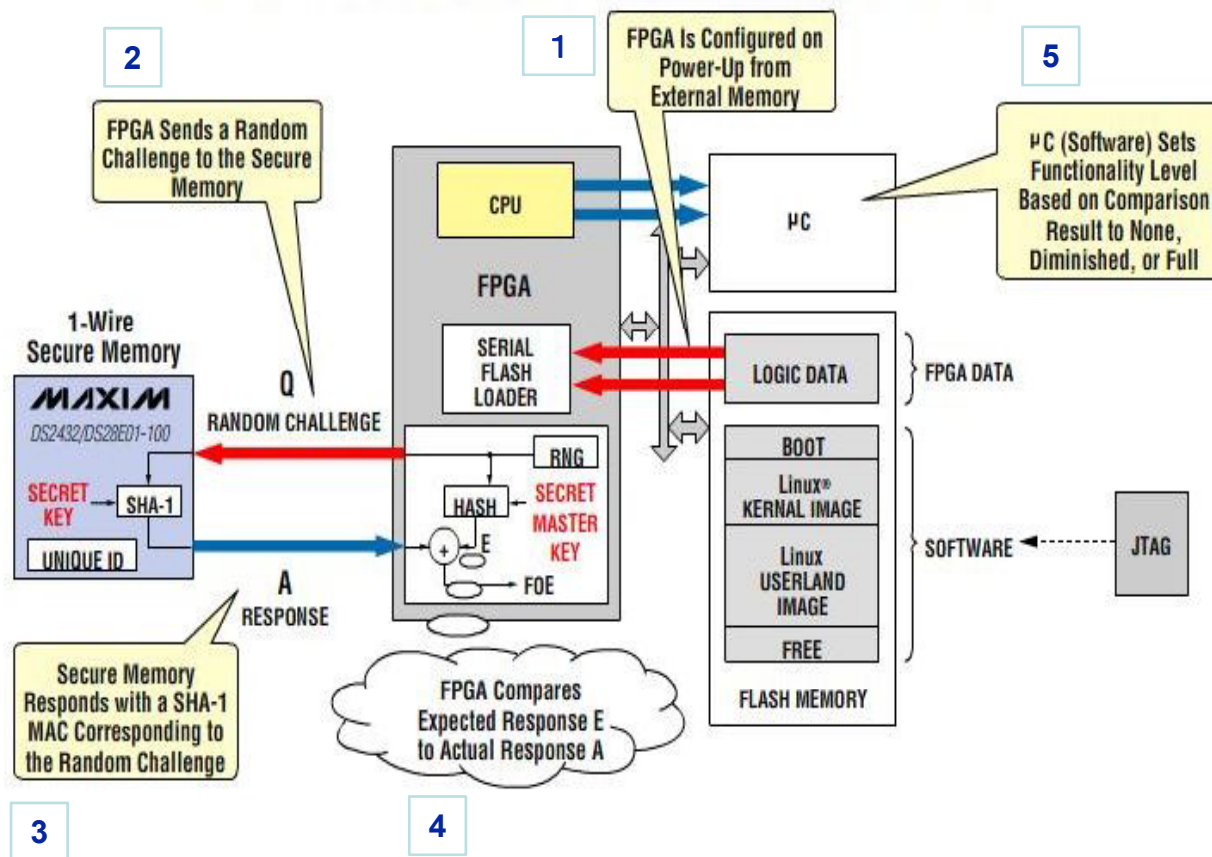
1-WireメモリによるFPGAセキュリティ

– なぜSHA-1を使うのか？

- パブリックプロトコル、国際的暗号コミュニティによって徹底精査
- FIPS認定(FIPS 180-1、180-2)
- ISO/IEC 10118-3仕様に適合
- 輸出規制EAR99対応で製品準備

1-WireメモリによるFPGAセキュリティ

コストが最適化されたコピー保護スキーム—IFF (敵味方識別装置)



1: FPGAは、電源立ち上げ時に外部メモリよりコンフィギュレーションされます。

2: FPGAは、ランダムチャレンジをセキュアメモリに送ります。

3: セキュアメモリは、送信されたランダムチャレンジのSHA-1 MACを返信します。

4: FPGAは、ホストで演算したレスポンスE と実際に返信されたレスポンスA を比較します。

5: μ C (ソフトウェア)は、比較結果によって基本機能レベルの動作不可、機能制限または、完全な使用の設定をします。

[参照：1-Wire FPGAビデオチュートリアル\(英語のみ\)](#)



参照アプリケーションノート

- [FPGA Design Security Solution Using Secure Memory: Alteraのリファレンスデザイン](#)
- [1-Wire SHA-1セキュアメモリによるXilinx® FPGAのIFFコピー防止](#)
- [SHA-1によるR&D投資の保護](#)
- [1-Wireとは？](#)
- [ソフトウェアを介した1-Wire®通信](#)
- [1-Wire製品ページ](#)

問い合わせ E-mail: Tech.Japan@maxim-ic.com