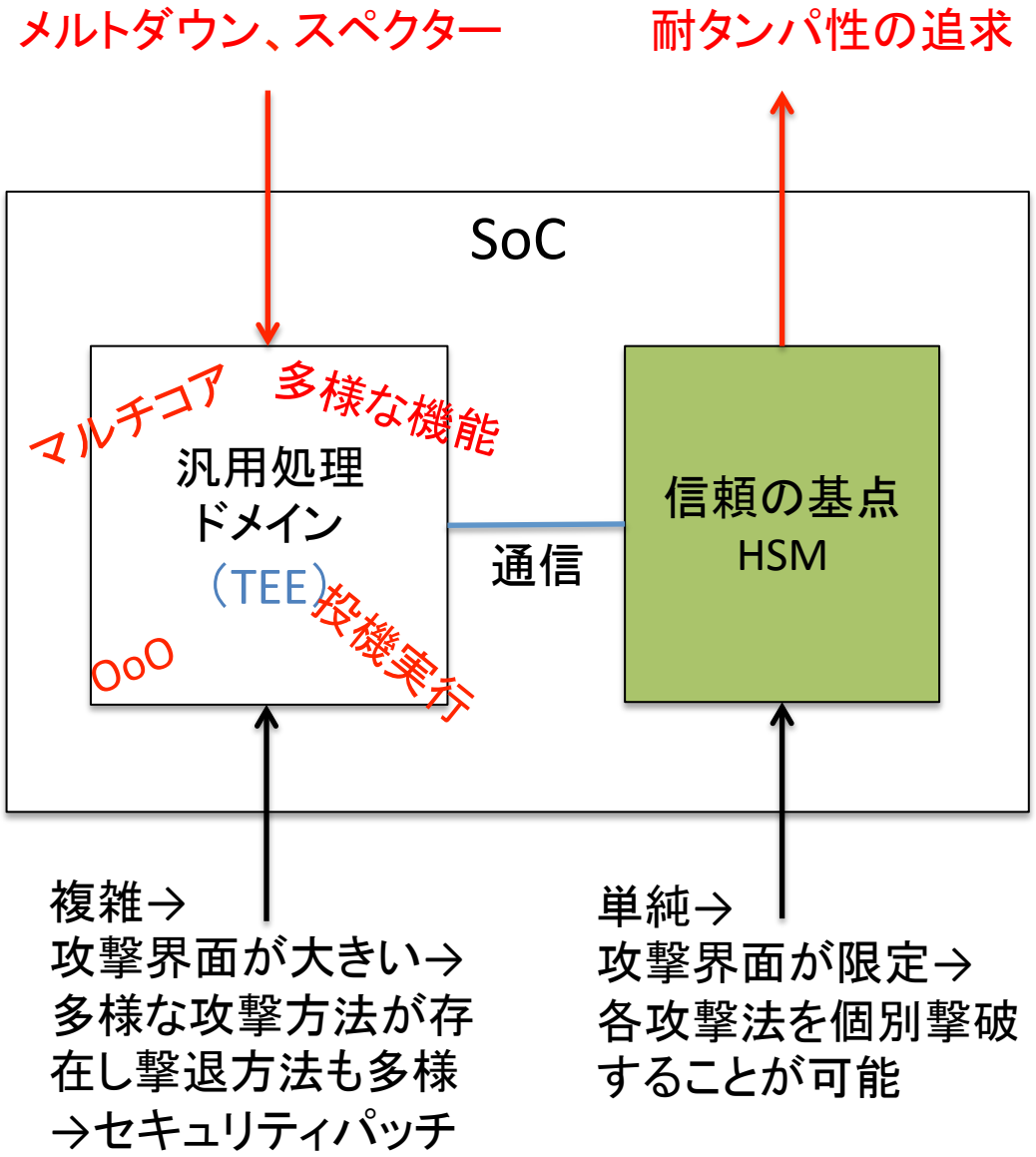
RISC-V IoT機器向けハードウエアセキュリティモジュール「クリプトスペック」

2019年09月27日

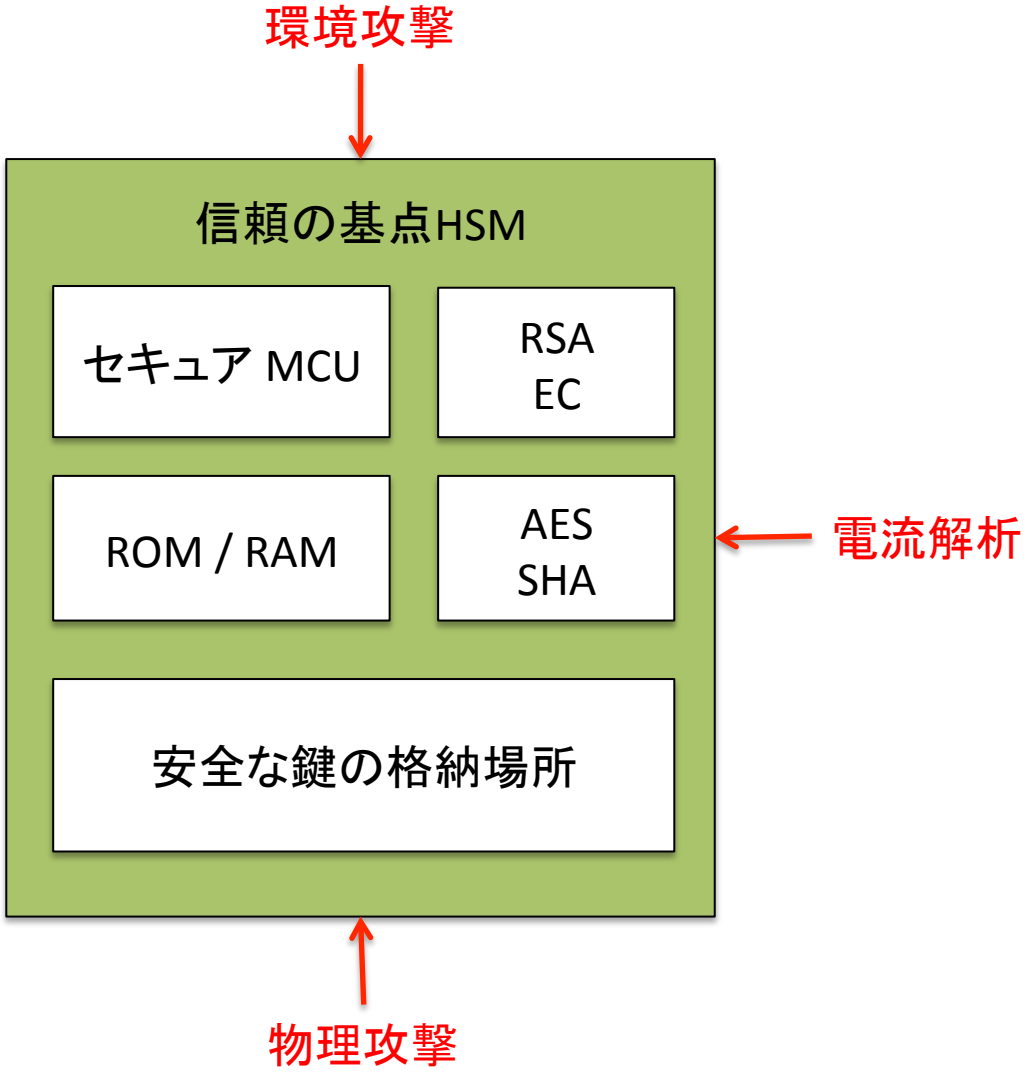
SHコンサルティング株式会社
河崎俊平

SoC用信頼の基点
ハードウエアセキュリティモジュール（HSM）



- 汎用処理ドメインを守ろうとするとシステムは複雑で、守る方法が特定できない。
- 信頼の起点を分離、単純なシステムを護る方が有効。
- スマホではルートオブトラストを基盤に保護層を数層創り、システム全体を護っている。

信頼の基点HSM
＝世界最小のコンピュータ



- 単純だから、アーキテクチャ、マイクロアーキテクチャ、論理実装レベルにハッキングされぬオリジナルな工夫を盛り込むことができる。

- RISC-Vを使うことで、上記の全部のレベルをスクラッチから設計できる。

信頼の基点HSM: 攻撃コスト対守備コスト

- 攻撃コスト例 > $25K /デバイス
- 守備コスト例 < 10¢ /デバイス = ハード実装＋初期固有鍵
- 攻撃方法をカテゴリ化し攻撃界面を全面網羅、安価な攻撃はがっちり対処。HSMサーバで鍵運用をモニタし漏洩鍵検出。ゼロ化。

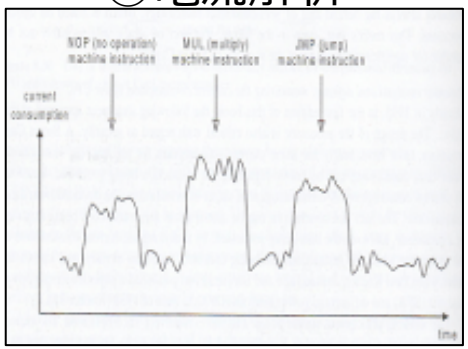
① サイドチャネル攻撃　→安価

=｛タイミング攻撃 | 電力解析 | 電磁波解析｝

②チップ開封型　→高価

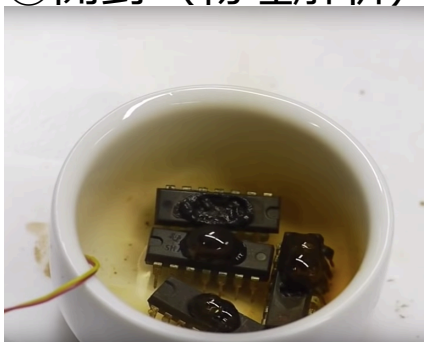
=｛プロービング解析 | マイクロプローブ | 光照射　| 発光解析 | FIB配線編集 | レイアウト再配置 | 保護回路破壊 | テスト回路復元｝

①電流解析



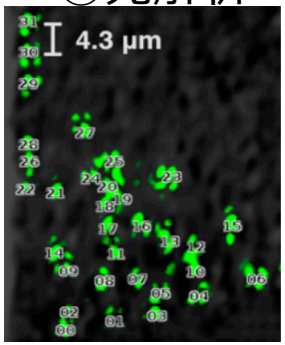
出典：https://elearning.renesas.com/pluginfile.php/354/mod_folder/content/0/Board_ID/BoardID_RI_training_NR_03112010.ppt

②開封（物理解析）

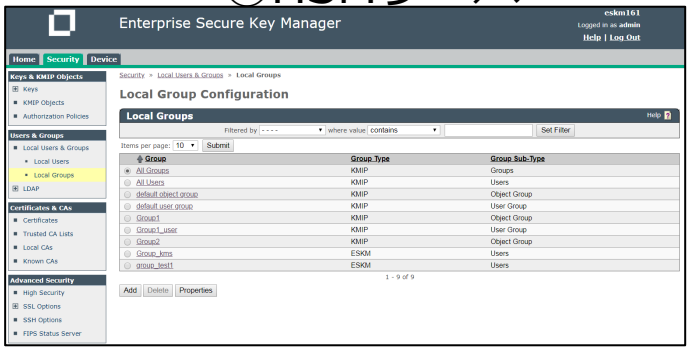


出典：　https://youtu.be/uAINV-VXuq0
https://eprint.iacr.org/2017/822.pdf

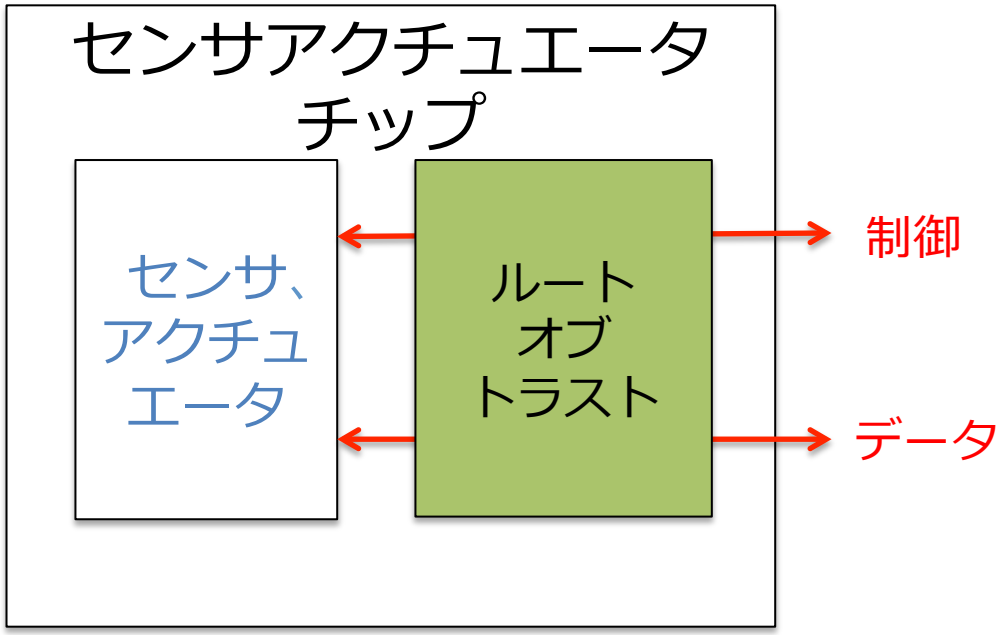
③光解析



④HSMサーバ



信頼の基点のセンサ/アクチュエータ応用

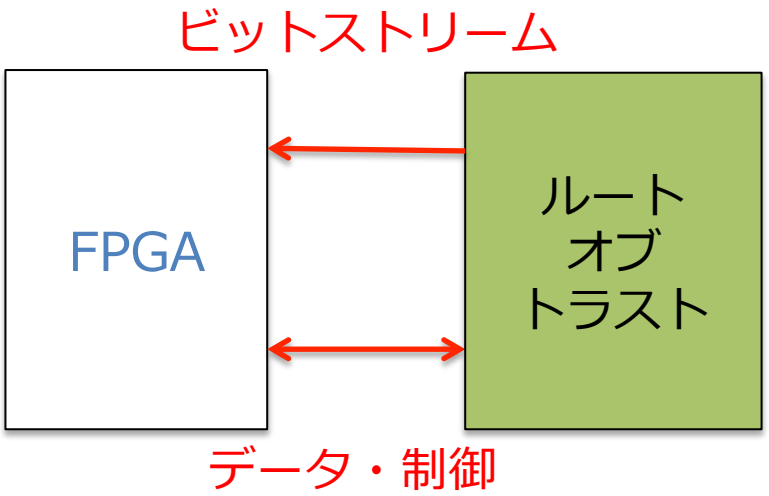


センサ、アクチュエータにも固有鍵に基づく信頼が必要。

ルートオブトラストがモニタするのは汎用処理ドメインとは限らない。センサアクチュエータも対象にできる。

- 汎用処理ドメイン以外に、センサアクチュエータにもルートオブトラストの組込みニーズがある。
  - 制御信号、データ信号がアセットで、これを暗号化して護るニーズがある。
  - センサ・アクチュエータが攻撃されていないかモニタ。例えば、周囲のデバイスが繋ぎ変えられていないか？
  - 攻撃を検出すると、アラート、システム立ち下げ、ゼロ化処理等を行う。
  - センサアクチュエータもネットにつながる。

信頼の基点HSMのFPGA応用

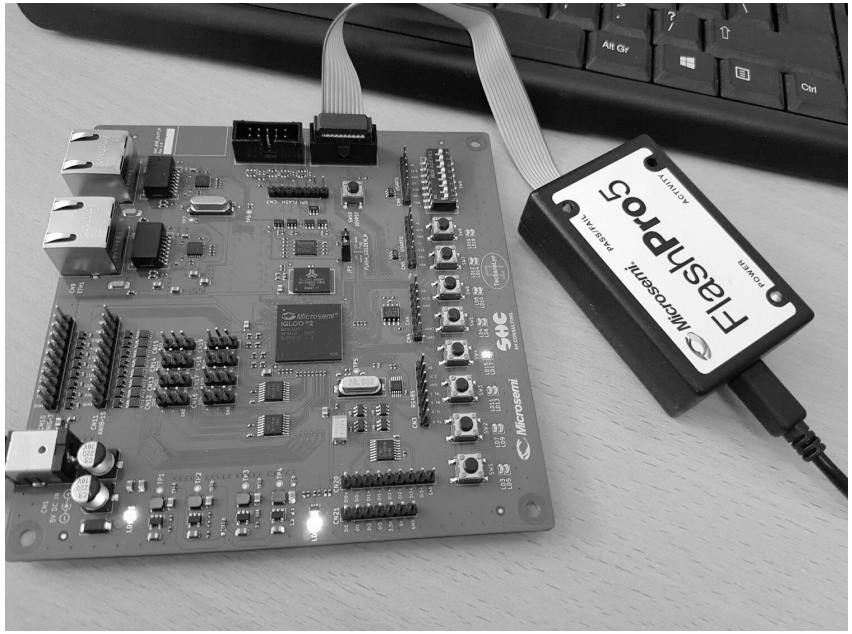


FPGAビットストリーム
仕様に従
ルートオフトラストから

FPGAビットストリーム
仕様は解明されている。

- 汎用処理ドメイン以外に、FPGAにもルートオブトラストの組込みニーズがある。
  - ビットストリームを暗号化して護るニーズがある。
  - FPGAビットストリーム仕様は解明されている。
  - FPGA部分再構成を使いセキュリティ性を増すことができる。

結論



- 信頼の基点HSMはリプログラマブルであるべきか？
- ハードとファームがミニマルだと、システム全体検証が可能。ROM品もありうる。
- FPGA上に32-bit RISC-Vを構築し信頼の基点HSMの検証を開始。
- OSを構築する。
- オープンソース版も作成し、組み込みを容易にする。

この成果の一部は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務の結果得られたものです。