ヘテロジニアスインテグレーション

ロードマップ

2019年度版

第19章: セキュリティ

http://eps.ieee.org/hir

HIR は、技術評価のみを目的として考案されており、個々の製品または機器に関連する商業上の考慮事項とは無関係です。

このロードマップでは、元のソースから抜粋した資料および図の使用に感謝します。

図と表は、元のソースの許可を得てのみ再利用する必要があります。

第19章: セキュリティ

エグゼクティブサマリー

半導体とそのアプリケーションのトレンドは、セキュリティと信頼性に課題をもたらします。一方、最先端のプロセッサは、ネットワークと通信、送電網、金融、軍事、航空宇宙システムなど、非常に重要なシステムとインフラストラクチャの背後にある「頭脳」です。一方、小型の組み込みプロセッサ、センサー、その他の電子コンポーネントは、自動車のブレーキシステムやエアバッグシステム、パーソナルヘルスケア、産業用制御、その他の接続デバイスの急成長リストなど、さまざまなアプリケーションで「スマート」な機能と接続性を提供します 多くの場合、モノのインターネットと呼ばれます。幅広いデバイスとアプリケーション、および接続された「モノ」の数の急激な増加により、セキュリティと信頼性が主な関心事になっています。

セクション1. 一般的なサイバーセキュリティハードウェアの課題とニーズ

サイバーセキュリティの脅威は、ソフトウェアまたはハードウェアを介して出現する可能性があります。脅威の大部分はソフトウェア攻撃によって発生し、電子メールの添付ファイル、偽のWebサイト、安全でないワイヤレス、ソーシャルネットワーキング、感染したUSBドライブなど、多くのソースからのアクセスを提供します。これらの攻撃は、通常、ソフトウェアの脆弱性を利用して、感染したシステムへの不正アクセスと制御を容易にします。他の攻撃では、通信インターフェイスを使用して、メッセージやソフトウェアの更新を偽造したり、プロトコル障害を挿入したり、メッセージをスパイしたり、中間者攻撃を使用して貴重な情報を入手したりします。これらの攻撃に対する緩和策は通常、これらの脆弱性に対処するソフトウェアアップデートのインストールを伴います。未知または制御されていないソフトウェアのソースを単純に回避することは、潜在的なウイルス保護ソフトウェアとともに、最も効果的な防止戦略です。これらのソフトウェアの脅威は通常、ハードウェアに固有のものではないため、HIセキュリティロードマップの範囲外です。一方、ハードウェアセキュリティの脅威は、チップのハードウェアコンポーネントの設計と統合、およびチップがパッケージレベル、ボードレベル、およびシステムレベルで機能システムまたはサブシステムに統合される方法に大きく影響されます。これらのハードウェア攻撃は、7つの大きなクラスに分類されます。インターフェイスのインターフェイスャネル攻撃、サイドチャネル攻撃、チップの偽造、システムの物理的な改ざん、フォールトインジェクション攻撃、リバースエンジニアリング攻撃です。表1は、これらのハードウェア攻撃クラスと、一般的に採用されている軽減戦略をまとめたものです。

Table 1. Hardware Attack Classes

ハードウェア攻撃ベクトル	影響	緩和戦略
インターフェイスリーク	インターフェイスで直接、またはテストメカニズム/インターフェイスを介した不正アクセス	セキュリティの設計、インターフェイスの難読化
サプライチェーン攻撃	隠された/遅延された不要な機能またはセキュリティの侵害（機密性、整合性、または可用性）、トロイの木馬など	設計の検証、寄生検出、テストまたは検証でのアクティブなトリガー。 IP /設計/材料の出所
サイドチャネル攻撃	電力、EM、タイミングなどのシステムシグネチャを観察することにより、暗号化キーなどの安全な情報へのパッシブアクセス	シミュレーションを通じてサイドチャネルリーク（タイミングベース、電力ベース、電磁的、音響的、光学的、熱的など）を分析し、デザイン変更によるリークをブロックすることにより、デザインをサイドチャネル耐性にする
チップ偽造	古くなったチップを無断で使用したり、複製したチップや妥協したチップを製造	安全なチップ走行距離計と物理的なクローン不可能な機能に基づく独自の認証
物理的な改ざん	リバースエンジニアリングを含む安全な情報への侵入的/半侵入的アクセス	侵入を検出してシステムを非アクティブにするセンサー
フォールトインジェクション攻撃	設計に実装されたセキュリティを回避することを目的とした制御フロー/データ整合性	実行の堅牢性とデータの整合性を向上させるために利用されるフォールトトレラントな方法
リバースエンジニアリング攻撃	ハードウェアとファームウェア（ROMコードとマイクロコードを含む）を検査して、機能要素とその相互作用を特定し、埋め込まれた秘密にアクセスし、脆弱性と弱点を見つけ、障害攻撃、物理的攻撃などの他の攻撃を開始します。 サイドチャネル攻撃、または物理的な改ざんまたはチップの偽造の方法を発見する	改ざん防止フィクスチャと、ブラインド/埋め込みビアまたはロジックロックなどのレイアウトの難読化。

ハードウェア攻撃の分類のための分類法が開発中であることに注意してください。図1は、物理攻撃の分類法（TrustHub [2]）を示し、詳細を左から右に示します。パッシブとアクティブです。 侵襲的、非侵襲的、または半侵襲的。 攻撃ベクトル、及び実際の攻撃タイプ。攻撃ベクトルの多くは表1にありますが、図1へのマッピングは1対1ではありません。

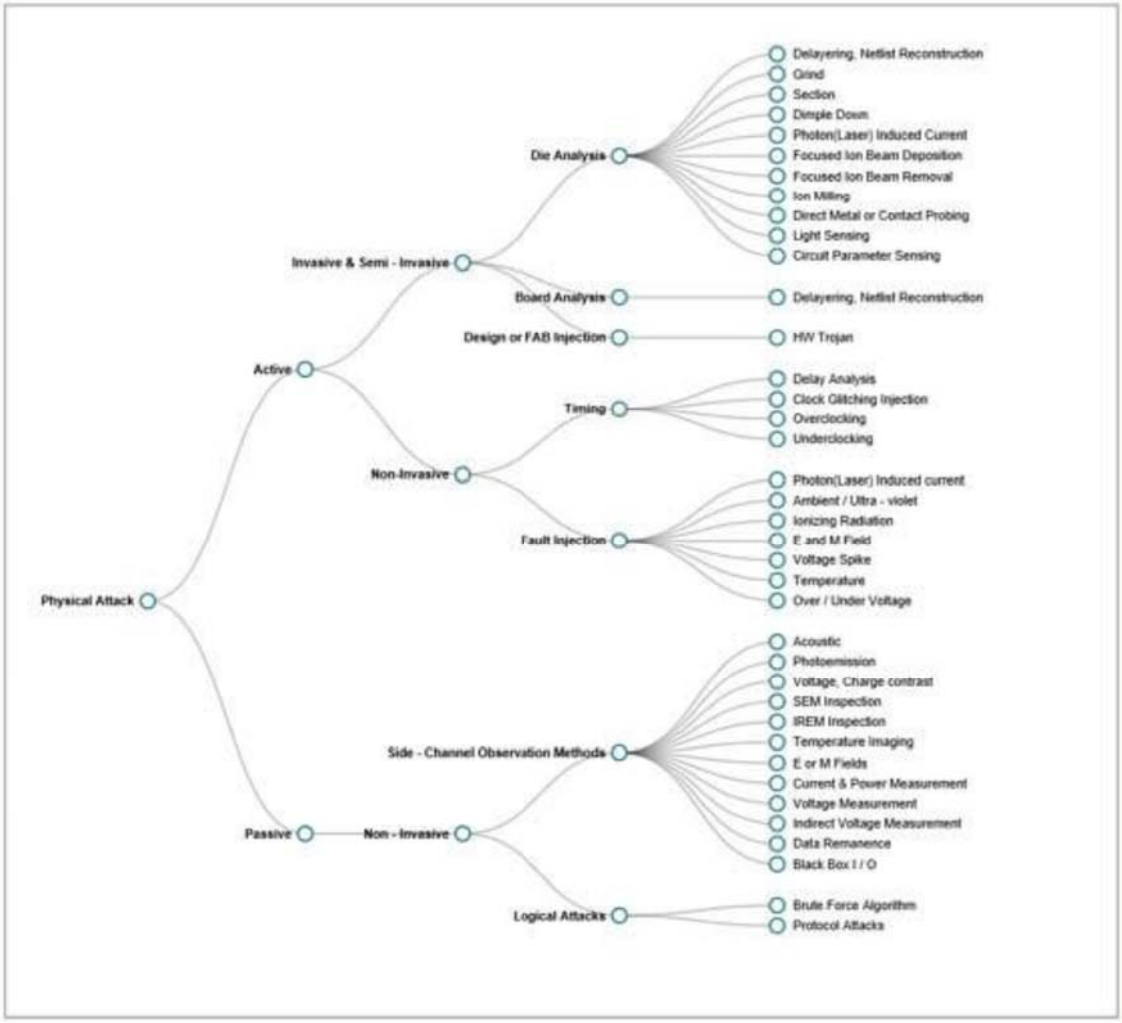


Figure 1. Taxonomy of physical attacks.[2]

今日の複雑な半導体回路とシステムの設計と製造には多くの手順が必要であり、通常は世界中の複数の場所や組織に分散している数百人のエンジニアの作業が含まれます。さらに、今日の半導体チップには、複数のソースからの設計モジュールまたはブロック（知的財産（IP）ブロックとも呼ばれる）が含まれている可能性があります。詳細な仕様は回路図に変換され（仕様をさまざまな抽象化レベルにマッピングすることにより、アーキテクチャ、ビヘイビア、マイクロアーキテクチャ、レジスタ転送、トランジスタ、デバイス）、数十億のトランジスタを含む物理設計に変換されます。多くのプロセスが開発されており、製品が意図したとおりに機能することを検証、テスト、検証するために、設計および製造パスに沿って多くのリソースが投入されています。ただし、これまでのところ、これらのプロセスは、不正なアクセスまたは制御を提供するようにチップが変更されているかどうかについて100％の信頼性を提供していません。このような望ましくない動作は、意図しないサイドチャネルをもたらす設計の弱点、または悪意を持って挿入された機能や「トロイの木馬」ハードウェアが原因である可能性があります。

セキュリティとセキュリティ検証のための設計への関心が高まり、ほとんどの大規模な半導体設計および製造会社は、セキュリティと検証のための設計を標準プロセスに組み込んでいます。主な焦点は、半導体回路とシステムが、後続のステップで検証、製造、およびテストを実行可能または簡単に行えるように設計され

ていることを確認することです。必要なのは、意図しない動作やアクセスの可能性を減らし、改ざんや偽造に対する抵抗力と回復力を高め、能力を向上させることを目的として、すべての半導体設計および製造会社によるセキュリティ設計の理解とそれに最大限の注意を払うことです。フィールドでの認証を提供します。セキュリティの設計には、アーキテクチャと仕様の戦略を含む新しいスケーラブルなソリューションと、特に正式な方法が現在弱いか存在しない設計段階での合成、物理設計、テスト、および検証のためのツールが依然として必要です。設計の初期段階を対象とした方法と手順は、より効果的で手頃な価格になる可能性があります。

脆弱性がなく、攻撃、さらには（まだ）知られていない脆弱性や攻撃に対しても確実で復元力のあるシステムを設計するために、ハードウェアセキュリティの理論的基盤を構築することが不可欠です。理想的には、そのような数学的モデルは脅威と応答の環境を抽象化し、（応答）近さ、安全性、脆弱性、攻撃などのシステムセキュリティのエンジニアリング概念を正確に形式化します。システムセキュリティを評価し、保証を定量化するためのメトリックは、そのような正式なモデル。既存および新規の自動化および設計ツールは、抽象化とメトリックを使用して、数値属性としてセキュリティプリミティブを指定し、設計中のシステムの他の設計プリミティブとのトレードオフを可能にします。

セキュリティソリューションの設計を成功させるには、システム設計者やメーカーからの競合する要求を考慮して、他の設計機能や考慮事項と統合する必要があります。例えば、システムの複雑さが増すにつれ、製造中および製造後および統合環境での可観測性と制御性の向上に対する要求により、サイドチャネル攻撃のリスクが高まります。オンラインのセルフテスト、リカバリ、適応、再構成を可能にする機能を設計すると、サイドチャネル攻撃のリスクも高まります。これらの設計および製造技術に関連するリスクは、慎重に調査し、緩和または中和する必要があります。これらのリスクを軽減するための学際的なチームの役割は、最も重要です。

半導体のセキュリティが今日直面している脅威と課題には、以下のものが含まれますが、これらに限定されません:

- 動作、レジスタ転送レベル（RTL）、論理レベルまたは物理レベルでの仕様、設計、または実装における不要な機能。不要な機能は悪意のある、または不注意なものである可能性があります。これには、不完全で曖昧な仕様または実装が含まれます。
- 機密情報の漏えいや攻撃に対する弱点につながるインターフェイスの依存関係。これには、時間に依存する動作や、外部信号へのタイムアウトの不適切な依存が含まれます。
- 半導体ベースの部品/製品の偽造。
- 機密データまたは制御機能への不正アクセス。これには、キーまたは機密の内部データと制御へのアクセスが含まれます。
- 悪意を持って挿入されたハードウェアトロイの木馬、および製造中など、設計サイクルのあらゆる段階で設計を改ざんするその他の形式。
- 動作中の電子回路の信号のサイドチャネルを介した観測。
- フォールトインジェクションによって動作中に電子回路を改ざんする。
- 機能的、論理的、または電気的なレベルでの改ざんに対する不十分な耐性の特定-特に、電力、熱、または放射線攻撃などの既知の改ざん方法に対する耐性。
- ハードウェア認証とフィンガープリント。
- IPブロックの検証と追跡、および改ざんの欠如を含む回路の起源。
- 機密情報を漏えいしたり、検証できないため攻撃に対して脆弱な外部コンポーネントへの依存。
- 実行時に整合性チェックを可能にする、セキュリティおよび/またはベースラインの正式で定

量化可能な仕様。

相互接続されたIoTデバイスの世界では、セキュリティの設計に関する焦点を絞った研究の必要性が高まっています。具体的には、これには、安全性、信頼性、安全性、信頼性、プライバシーを保護するチップ、ならびにコンピューティングおよび通信システムの設計、分析戦略、プロセス、およびツールを開発するための研究が必要です。この研究では、意図しない動作やアクセスの可能性を減らし、改ざんに対する抵抗力と回復力を高め、サプライチェーン全体と現場で認証を提供する機能を改善する必要があります。
以下のトピックは、IoTセキュリティスペースの関連する研究領域の代表です:

- アーキテクチャと設計。ハードウェア固有のセキュリティプロパティを推論および指定するためのアプローチ、モデル、およびフレームワーク。これらの設計とアーキテクチャのアプローチを個別に検討するべきではありません。回路とプロセッサのレベルでのセキュリティの影響は、システム全体の機能、パフォーマンス、および電力の目標の観点から理解する必要があります。
- 原則、プロパティ、およびメトリック。ハードウェアセキュリティ設計の原則と半導体固有のプロパティ。設計を評価または比較するためのセキュリティメトリック。拡張可能であり、プライバシーの構成やシステムレベルでの信頼の証拠の提供に役立つ可能性があります。
- 検証。ハードウェア固有のセキュリティプロパティを確認し、セキュリティ設計原則を実施するためのツール、手法、および方法論。設計のすべての側面を知らずに安全特性を確立する革新的なアプローチ。これにより、証明可能な強力な保証が提供されます。セキュリティの検証と分析の自動化を高めるためのアプローチ。
- 組み込みソフトウェアとファームウェア。組み込みソフトウェアとファームウェアの脆弱性を減らし、フィールドでの展開後に発見された既知の脆弱性に対処するためのアップデートを提供するための保証戦略と手法。
- 認証と証明。設計中およびライフサイクル全体で検証可能なアーチファクトまたは設計要素を挿入するためのモデル。ハードウェアで実装されたキーの生成、保護、信頼モデルの確立などのサポート問題にも関心があります。

セクション2. 特定のHIセキュリティニーズ

特定のヘテロジニアスインテグレーションサイバーセキュリティ研究のニーズ

IC設計、パッケージング設計、セキュリティ設計の世界は、ヘテロジニアスの統合イニシアチブと融合しています。ファンアウトウエハーレベルパッケージ（FOWLP）、シリコンインターポーザー、ウエハーオンウエハー（WoW）、パッケージオンパッケージ（POP）、3D IC、2.5D IC、再配線層付きファンアウト（FO）などの新しいテクノロジー(FO w RDL）は、個々の要素だけでなく、システム全体のセキュリティを最適化するために、多くのICおよびパッケージサプライヤが協力することを要求します。セキュリティの設計と検証には、従来のセキュリティツールと方法論では解決できない独自の課題があります。非常に高いレベルで、ヘテロジニアスインテグレーションは3つの基本的なセキュリティリスクを悪化させます。1）広範なサプライチェーンからの多くの多様なチップを使用します。2）これらのチップを共有リソースとの物理的接触をはるかに近くして、サイドチャネル攻撃の脅威を増大させます。悪意のあるチップ、3）通信帯域

幅、接続性、これらのチップ間の脆弱性が増加します。

特に、HIの潜在的な攻撃面の増加は最初は否定的に見ることができますが、適切な設計洞察はシステムのセキュリティを大幅に向上させることができます。さまざまなシステムコンポーネント間での分割製造、強化されたサイドチャネル攻撃対策、強化された認証、階層型セキュリティアーキテクチャ、システムレベルの設計ツールなどの概念は、セキュリティを大幅に向上させることができます。設計ハウス、OSAT、ファウンドリ、OEM、EDAベンダーを、ICドメインとパッケージングドメインの両方で動作できるセキュリティツールと統合することにより、高度なHIシステムは、固有のセキュリティ脆弱性を大幅に削減できます。ヘテロジニアスの多くの側面が、システムのセキュリティに大きな影響を与える可能性があります。 HIの適用範囲は非常に広いため、これらの影響すべてを詳細に説明することはできません。表2は、他の各HIR TWGとの関連に基づいて、これらの影響を簡単に特徴付けしようとしています。

Table 2: First order security impacts of HIR TWG

関連HIR TWG	一次セキュリティへの影響
シングルチップとマルチチップのパッケージ	追加のインターフェイス、情報フロー、認証および機密性の懸念
統合フォトニクス	光ファイバーのサイドチャネルアタッチメント（SCA）は、EM SCAの場合よりも近接している必要があります。
統合パワーデバイス	よりローカルな規模でのDP SCAはより困難ですが、潜在的には情報量が多くなります
MEMSとセンサーの統合	コンテンツ
RFおよびアナログ混合信号	ローカルセンサーの統合により、改ざんやリバースエンジニアリングをより適切に阻止できる
材料および新興研究材料	ワイヤレス通信とワイヤレスアップデートによる主な影響
新興デバイス	磁性材料の統合により、EM信号のシールドが向上
相互接続	キュービットと絡み合った通信は新しいセキュリティパラダイムを設定することができ、スピンベースのデバイスは追加のエントロピーを持っています
テスト	チップの相互接続性と脆弱性に対する主な影響（以下を参照）
サプライチェーン	安全な設計のない柔軟なテスト方法は脆弱性を悪化させます（以下を参照）
SiP	複数のチップの複数のサプライヤーは、新しいインターフェイス制御を必要とします（以下を参照）
3D + 2.5D	さまざまなサプライヤーのチップの近接性と接続性の向上により、リスクが増大します
WLP	チップの近接性とSCAに対する脆弱性への主な影響（以下を参照）
モバイル	さまざまなサプライヤーのチップの近接性と接続性の向上により、リスクが増大します
IoT	システム更新のための無線通信はリスクを増大させます
医療と健康	さまざまなサプライヤーのチップの接続性の向上により、リスクが増大します
自動車	生命を脅かすリスクには、セキュリティのパーティション分割とセーフモードのデフォルトの増加が必要です（以下を参照）
高性能コンピューティング&	生命を脅かすリスクには、セキュリティのパーティション分割とセーフモードのデフォルトの増加が必要です（以下を参照）
データ	高いチップ間帯域幅は、独自のセキュリティスクリーニングの課題をもたらします
航空宇宙および防衛	生命を脅かすリスクには、セキュリティのパーティション分割とセーフモードのデフォルトの増加が必要です（以下を参照）

相互接続

ヘテロジニアスインテグレーションは、主に、携帯電話、時計、医療機器など、さまざまな機能をより小さなフォームファクターに統合する必要性によって推進されます。まず、このコンパクションには、相互接続の長さを短縮し、関連する電力とレイテンシの両方のスケーリングを削減するという直接的な利点があります。関連するチップの数も一般的に増加しており、チップ間の安全なインターフェイスが必要です。相互接続密度の増加に向けたさらなる推進により、システム内のさまざまなチップ間の帯域幅の接続性が向上し

ました。WLPなどのいくつかのHIプロセスオプションは、追加のファンアウト再配布レイヤーも提供します。

セキュリティの観点からは、これらの変更のほとんどは悪影響を及ぼします。チップインターフェイスの数の増加とチップ間の帯域幅の増加は、攻撃対象のより多くのコンテンツとより豊富なコンテンツの両方を提供します。チップ同士がより接近し、チップ間の帯域幅接続が潜在的に高くなると、サイドチャネル攻撃のリスクが高まります。HIインターコネクトスケーリングの唯一のセキュリティ上の利点は、短いインターコネクトラインのより小さい電磁気（EM）と差動電力シグネチャ、及びEMシグネチャを抽出するために必要な細かいスケールと近接プローブに関連しています。

テスト

多くの異なるサプライヤーの多数の多様なチップを柔軟かつ効果的にテストできるようにすることは、適切なテスト用設計アルゴリズムとセキュリティ用同時設計アルゴリズムが採用されていない場合、大きなセキュリティ上の課題となります。テストで使用されるスキャンチェーンは、最も効果的な攻撃対象としてよく使用されます。HIテストでは、これらのリスクを最小限に抑えるために、十分なパーティション分割と制御の変更が必要になります。これは、共有リソースをテスト時に効果的に分割できない場合に特に重要です。

サプライチェーン

ヘテロジニアスは、多様な機能と多様なコンポーネントサプライヤーの両方を意味します。これらの変更はどちらも、システムのセキュリティに本質的な課題をもたらします。 この多様な機能は、特にそれが多様な機能セットのテストに関連しているため、より高い柔軟性とインターフェイスでのセキュリティの露出を必要とします。明らかに、さまざまで多様なコンポーネントサプライヤーの数の増加は、悪意のあるチップの潜在的な数を増やすだけでなく、これらのインターフェイスでセキュリティベースの標準化を実装してこれらのリスクを減らす必要性を高めます。これらのインターフェイスの標準を確立することは、HIに基づく信頼性の高い製品の将来に対する主要な課題の1つです。

2.5D および 3D

第一に、2.5Dと3Dの両方の処理は、HIインターコネクトの進化の一般的なトレンドを拡張したものであり、チップをより大きなチップ間帯域幅でより近くに配置します。ただし、2.5Dと3Dの両方、および他のいくつかの垂直統合アプローチでは、ダイを互いに直接接触させるという基本的な幾何学的変化があります。これには、システムセキュリティの利点と欠点の両方があります。

ダイ間の直接接触により、スタック内の悪意のあるチップからのサイドチャネル攻撃のリスクが大幅に増加します。特に、スタックに挿入されたスパイチップは、そのすぐ上と下のチップからEM、熱、電力のシグネチャを抽出する際に、感度と空間分解能が桁違いに向上します。この脅威は、設計とシールドの両方の緩和戦略で対処する必要があります。垂直スタックのセキュリティ上の利点には、適切に垂直に挿入されたシステムセキュリティ制御チップがあり、分散された2Dジオメトリよりも効果的な分離を提供できるため、通常、外部SCA署名が削減されます。

生命を脅かすリスクのあるアプリケーション

医療、自動車、航空宇宙、防衛などのいくつかのHIアプリケーションは、セキュリティ侵害に対して生命にかかわる結果をもたらす可能性があります。これらの特定のアプリケーションでは、セキュリティと高い

信頼性のために、はるかに厳しい要件があります。特に、システムの監視、動的な応答、及びセキュリティ攻撃を軽減するためのパーティション分割は不可欠です。さらに、システムは、常に安全な状態で動作できるように、高い信頼性が得られるように基本的に設計する必要があります。このような設計要件は単なるセキュリティ上の脅威を超えていますが、これらの脅威は動的で予測不可能な性質のため、特に注意を払う必要があります。

協調設計

上記で何度も言及したように、HIのセキュリティ問題の大部分に対する提案されたソリューションは、単にセキュリティの設計として述べられています。HIセキュリティの真の課題は、上記の特定のHIセキュリティリスクに対処する一貫したセキュリティ設計アプローチが現在存在しないことです。特に、HIには、複数のチップやメーカーにまたがる新しいシステムレベルの設計パラダイムが必要です。EDAコミュニティは、独自のHIニーズのいくつかに対応するシステム設計ツールの開発を始めたばかりですが、現在はセキュリティにほとんど注意を払わずに、機能とパフォーマンスに焦点を合わせています。以下の分割製造のセクションで説明するように、このようなシステムレベルのセキュリティ設計アプローチによって実現できる多大なセキュリティ上の利点があります。

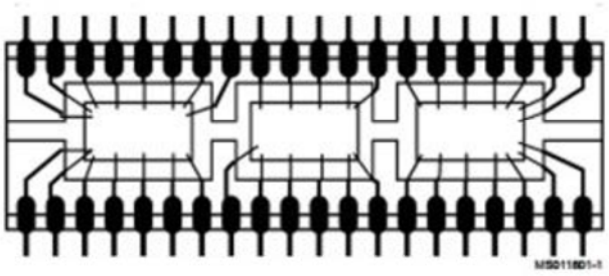
セクション3. 特定のHIセキュリティの機会

A. 情報の流れと認証

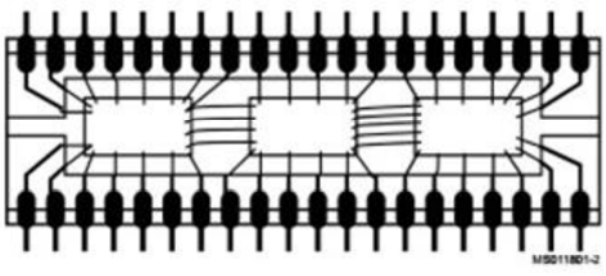
このセクションでは、パッケージにカプセル化された統合された異種システムのセキュリティを向上させるために使用できる手法をまとめています。サブセクション1では、ヘテロジニアスインテグレーション（HI）システムの業界で使用されるいくつかの一般的なパッケージタイプを紹介します。サブセクション2および3では、HIシステムの情報フローを保護する手法について説明し、サブセクション4では、パッケージ化されたICの認証に関するいくつかの手法について説明します。これらは、サプライチェーンのセキュリティの観点から重要です。

1. 複数のチップパッケージタイプ

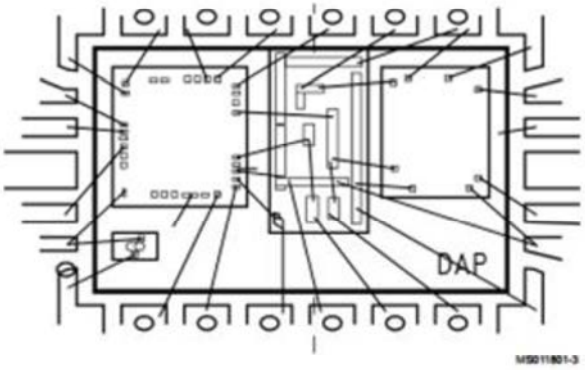
今日の集積回路（IC）は、同じまたは異なるプロセスで設計、検証、製造された小さなシステムのネットワークとしてより複雑なシステム（または大きなシステムのサブシステム）を設計する柔軟性を提供するため、パッケージで複数のダイを使用する場合があります 、テスト済み。 図3は、パッケージ内のダイの可能な統合方法のいくつかを示しています。セキュリティの観点からは、ダイを接続するネットワークにいくつかのセキュリティ要件を課す必要がある場合があります。これは、ネットワークが攻撃をプローブするために攻撃者によるはるかに簡単なアクセスに情報を公開するためです。



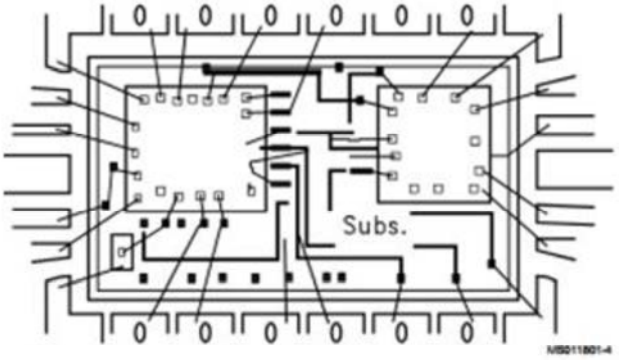
Type 1: Multiple die with die-to-leadframe bonding. No substrate. [3]



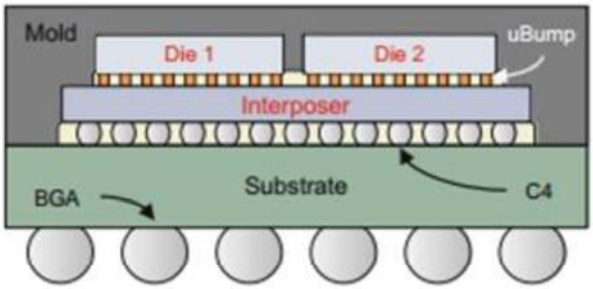
Type 2: Multiple die with die-to-die bonding. No substrate. [3]



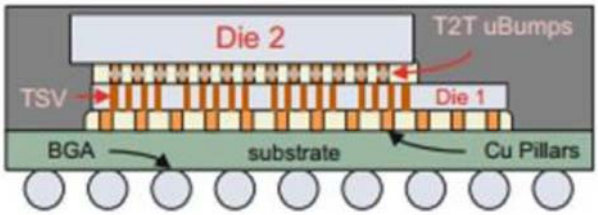
Type 3: Multiple die with jumper chip. No substrate. [3]



Type 4: Multiple die on substrate. [3]



Type 5: Multiple die in 2DS architecture. [4]



Type 6: Multiple die in 3D architecture. [4]

Figure 3. Multiple package types

2. パッケージ内のチップ間の情報フローの保護

図4に、ダイAとダイBを接続するバスを示します。これにより、ダイ間の情報交換が可能になります。ここでバスはデータと制御信号の両方を含みます。この図は図3のタイプ4に基づいていますが、2つのダイが相互接続によって接続され、それらの間の情報交換を可能にすることのみを目的としています。AおよびBは、タイプ4の水平相互接続の代わりに垂直相互接続を持つタイプ5（2.5D HI）およびタイプ6（3D HI）のダイを参照することもできます。情報フローを保護する手法は、すべてのタイプに適用できますが、タイプ例として4を使用しています。

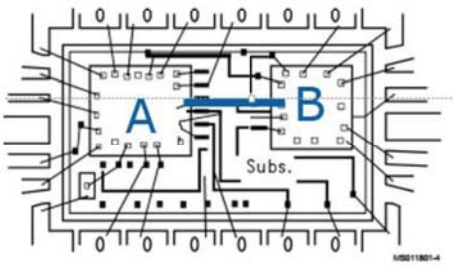


Figure 4. Inter-die information flow between dies A and B [3] with some modifications

プローブ攻撃が暗号化されたデータの機密性を損なわないことを保証し、プローブ攻撃を軽減するには、機密性要件のある信号が暗号化されたダイ間を通過する必要があります。バイパス攻撃またはデータインジェクション攻撃（Man-In-Middle攻撃）が検出されずに送信側ダイから受信側ダイに送信されるデータを変更できないようにするには：

- 整合性要件のある信号は、ハッシュベースのメッセージ認証コード技術を使用して、ダイ間を通過する必要があります。
- 完全性と機密性の両方の要件を持つ信号は、認証された暗号化プロトコルを使用してダイ間を通過する必要があります。

3. 物理的攻撃に対するセキュリティを向上させる手法

代替または補完的な方法として、次の手法を使用して、パッケージが開かれたか、プローブ攻撃が試行されているかを検出できます:

- チップが開梱されたことをシステムのセキュリティ制御/監視ユニットに通知するために、アンチテンパーセンサーを設計してダイに実装する必要があります。センサー：光センサー、圧力センサー、静電センサーまたは電磁センサー。
- アクティブシールドとパッシブシールドを設計してダイに実装し、攻撃のプロービングを回避できます。
- ダイで使用されるワイヤー相互接続のサブセットは、分割製造技術と同様のパッケージで設計できます。このような手法を使用すると、デパッケージによってパッケージを通過する相互接続サブセットが破壊され、機能しなくなる可能性があります。（パッケージをリバースエンジニアリングすることにより、相互接続のネットワークを決定できますが、この方法により、デパッケージ攻撃に対するセキュリティレベルが向上します。）

4. パッケージを認証する手法

サブセクション3.2および3.3で説明されている方法は、サプライチェーンのセキュリティの観点からマルチダイパッケージの情報フローのセキュリティに焦点を当てていますが、以下で説明されている方法は、一般にパッケージの認証に使用されます。私たちの焦点は複数のダイを持つパッケージにありますが、この方法は単一のダイを持つパッケージにも適用できます。

- パッケージに印刷された透かし。これは、最低のコストと最低のセキュリティで長い間使用されてきた最も古い方法です。
- パッケージのエッチングされたマーキング。
- デジタルホログラフィック透かし。[5]
- パッケージに独自のナノ構造を堆積またはエッチングする。[6]
- 物理的なクローンできない機能に基づく認証コード（パッケージ上に存在する一意のランダ

ムナノ構造）。

後者の4つの手法は、サプライチェーン攻撃に対するパッケージの堅牢性を高めるために考案されました。

B. 階層型/階層型セキュリティ

信頼できないサプライヤーからの集積回路（IC）とシステムオンチップ（SoC）のヘテロジニアスインテグレーションにより、システムインパッケージ（SiP）がサービス拒否（DoS）攻撃または暗号化キーなどの貴重なデータへの不正アクセスにさらされるまたはセンサーの読み取り値から派生したメタデータ。このような攻撃への対策は、常時オンまたは脅威によってトリガーされるものに大別できます。後者の場合、システムは最初に攻撃を受けていることを検出してから対策を有効にする必要があります。

巧妙な攻撃者は、ダイの製造プロセス中にハードウェアトロイの木馬を挿入した可能性があります。後でそれをトリガーするメカニズムを含みます。おそらく、盗む価値のあるデータの可用性に応じて、または高度計や温度計などのパッケージ内センサーからのデータに応じてです。設計検証または製造後のテスト中にトロイの木馬を検出するさまざまな方法が公開されていますが[7]、デバイスがフィールドに展開されるまで検出を回避できるほど十分に隠されていると想定する必要があります。したがって、SiPのサブシステムSoC内およびサブシステムSoC間で異常な動作を検出するためのアルゴリズム、およびSiPの信頼できるダイで実行されているセキュリティ監視ソフトウェアによってこれらのアルゴリズムを実装する方法を研究する必要があります。この信頼できるダイは、他のミッションクリティカルな機能を担当する場合があります。例えば、動的電圧および周波数スケーリング（DVFS）を制御して、バッテリーやエネルギーハーベスティングデバイスから電力を供給されるシステムなど、エネルギーに制約のあるシステムの稼働時間を延長できます。セキュリティコントローラー（SC）は、進行中の攻撃の検出への応答として、またはダイの信頼性を確立できない場合の事前対策として、各コンポーネントダイの電源レールへのアクセスを制御できる必要があります。または、SCは疑わしいダイをパッケージレベルの相互接続から隔離し、脅威のさらなるテストまたは評価が完了するまで、実質的に隔離下に保持することができます。1つのシナリオでは、セキュリティチェックが完了するまで、疑わしいダイの電源を入れたままにしておき、電源接続を維持するか、強制的に電源オフイベントを強制するかを決定する場合があります。

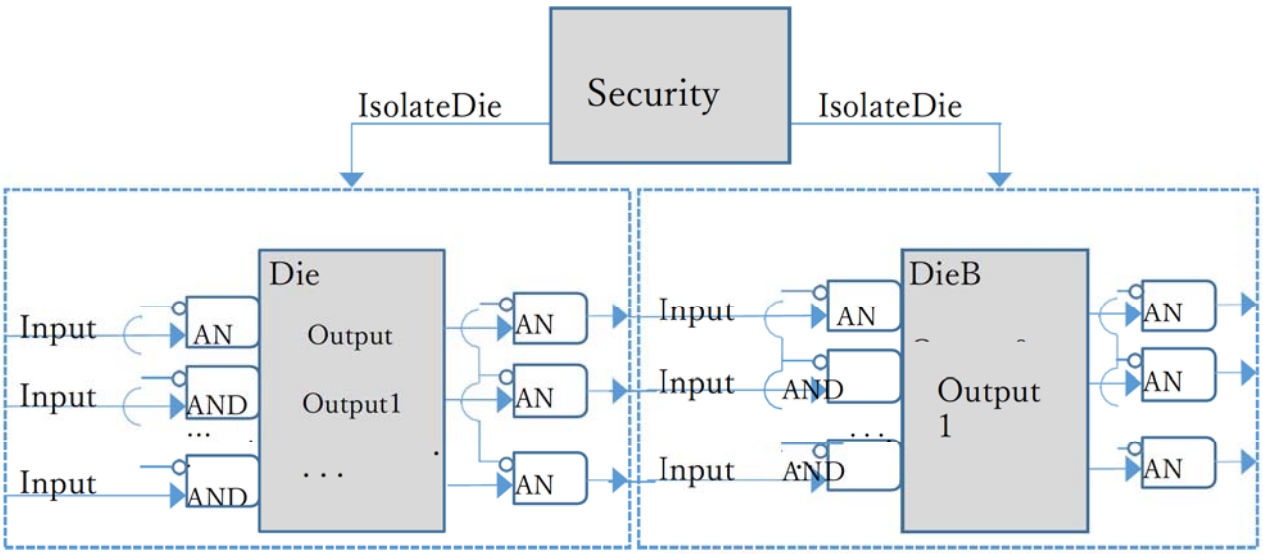


Figure 5: Die-level Isolation using a Security Controller

一般的なケースでは、ダイとダイおよびダイとシステムの接続性のテストには、各ダイの入力/出力/双方向ピンを外向きに構成する機能が必要になります（例えば、IEEE 1149.1のEXTESTモードの場合）。そのため、SiPに既に設計されているDesign for Testability（DFT）ハードウェアを利用して、各コンポーネントのダイを分離することが可能でなければなりません。スタック型集積回路用に開発されているIEEE標準であるP1838 [8]は、ダイを機能的に分離するための十分な制御性を提供する可能性がありますが、P1838準拠の分離ロジックが特別なテストモード以外で実際に利用できるとは限りません。セキュリティ脅威の識別に応じて分離ロジックを使用する場合は、セキュリティコントローラーが制御信号の正しいシーケンスを生成する機能を検証中にチェックする必要があります。さらに、ダイ分離回路は、悪意のある使用から保護する必要があります。たとえば、1つ以上のダイを分離してシステムを動作不能にするサービス拒否（DoS）攻撃などです。暗号化キーが提供されない限り、コントロールレジスタのセグメントへの書き込み（または読み取り）を防ぐために、ロックセグメント挿入ビット（LSIB）が提案されています[9]。

SiP設計者は、データトラフィックが予想される短い期間に、ダイ間通信ネットワークへのアクセスのみを許可することを好む場合があります。アクセスを許可/拒否するメカニズムは、図5に示すような単純な分離フェンスであり、制御入力信号はSCによって生成されます。SiP設計者は、パッケージレベルのインターコネクトのテストを有効にするためにオーバーライド機能を含めることができます。ただし、オーバーライドビットの設定は、暗号化認証が渡された場合にのみ実行でき（例えば、正しい暗号キーが提供されている場合）、暗号キーはSiPインテグレーターだけが知っています。

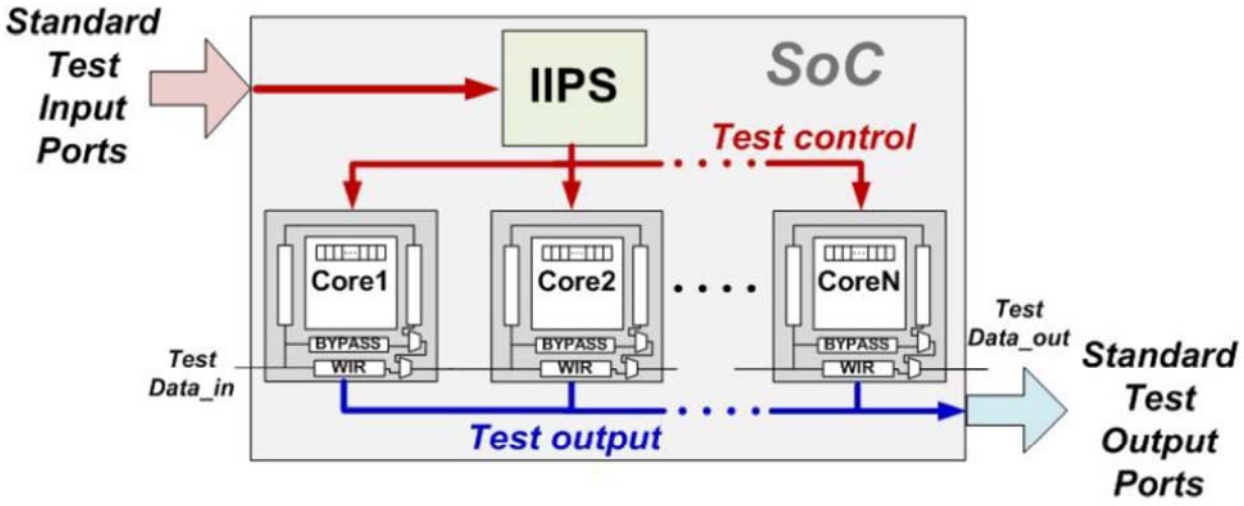


Figure 6: IIPS infrastructure IP for security interfaces with constituent cores of an SoC.[10]

次の図では、図6に示すように、SoCセキュリティ（IIPS）[11]のインフラストラクチャIPで、SCと同様の機能を持つセキュリティコントローラーが提案されています。HIでは、提案された概念を拡張できますが、違いは、（a）複数のダイがあり、（b）1つのダイが残りのダイを認証し、それらの間の安全な通信を提供することです。ただし、セキュリティコントローラーを偽造ダイと交換できないようにするメカニズムが必要であり、セキュリティに関してユーザーに誤った保証を与えます。

SCは、既知の長さおよび既知の入力データのアルゴリズムを完了するために必要なクロックサイクル数（または消費されるエネルギー）などのメトリックを使用して、SiPのサブシステム（IC / SoC）の動作を記述するメタデータを計算できます。このような既定のテストシーケンスの背後にある考えは、サブシステムがトロイの木馬がトリガーされた後に著しく異なるメタデータを生成する可能性があるため、定期的な間隔で行われた以前のテストの履歴データをSCに保存する必要があるということです。

システム設計者は、疑わしいトロイの木馬を含むダイによって生成されたデータに無効の可能性があるというフラグを付けることを好むかもしれません。疑わしいダイは、データに汚染の可能性があるというフラグが付けられることを除いて、通常どおりデータ値を送信し続けることができます。次に、複数のSiPから収集されたデータをコンテキストで評価できるため、サブシステムが本当に侵害されているかどうかを判断できます。各SiPのSCからの履歴メタデータを保存および分析し、命令をSCに送り返すことができます。例えば、缶詰テストシーケンスをより頻繁に実行できます。

C. 分割製造コンセプト

図7に示す分割製造の概念は、2つの異なるファウンドリ、つまり安全でないフロントエンドファウンドリと安全なバックエンドファウンドリの間でウェハ製造プロセスを分離することにより、シリコンチップの機能を難読化するために開発されました。多くの最先端のフロントエンドファウンドリがセキュリティレベルが低下して世界中に分散しているため、このアプローチはますます重要になっています。 ウェハレベルの分割製造で使用されるアプローチは、ピンの割り当て、セルの配置、および再ルーティングを変更して、チップの機能と脆弱性をいずれかまたは両方の製造元から非表示にすることです。

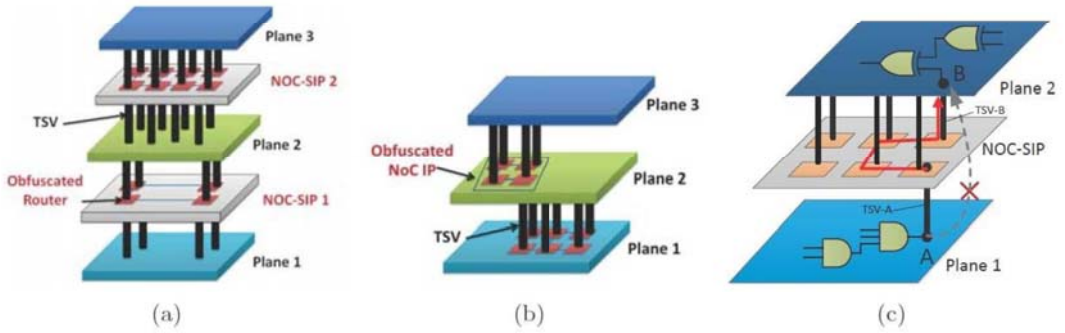


Figure 7: Concept of split manufacturing for security in a 3D stack.[12]

ICの世界での分割製造には、高いオーバーヘッドが必要です。上部のいくつかの金属層の非常に破壊的で費用のかかる分割と、異なる半導体ファブ間の基礎となるプロセスフローです。この分割は不自然であり、さまざまなファブでのハイブリッドフローに多くの追加コスト、テスト容易性の懸念、及び歩留まりの所有権の問題をもたらします。その性質上、パッケージレベルでの異種統合はこれらの懸念のほとんどに対処する必要がありますが、これまでのところ、HIパッケージレベルで分割製造コンセプトを使用してセキュリティを強化するために利用できる膨大な機会についての研究はほとんどありません。特に、セキュリティのために適切に設計されている場合、HI分割製造は2つのメーカー間での分割だけでなく、コスト、面積、またはテストの複雑さをほとんど増加させることなく、12の異なるチップコンポーネント間でセキュリティを分割できます。重要なのは、システムインテグレーターだけが知っている適切な暗号化キーとインターフェイスを使用して、さまざまなチップメーカーすべてでHIのセキュリティを設計することです。テストを容易にするために、必要なチップ間で限られたライフタイムキーを提供できます。

まず、セキュリティのためのHI分割製造設計では、追加のオーバーヘッドコストなしで、ICの分割製造の概念を使用できます。例えば、各チップサプライヤは柔軟なピンの再ルーティングを有効にできます。これらの暗号化されたピン割り当てキーは、最終的なシステムインテグレーターのみがアクセスできます。IC分割製造では2つのインターフェイスだけではなく、システム全体で12の異なるインターフェイスでこのような難読化を行うと、これらのシステムのリバースエンジニアリングやハッキングがはるかに困難になります。また、多くのサプライヤー、インテグレーター、EDAツールベンダー間のセキュリティ設計のための緊密な

協力も必要です。これは、ロードマッピングアクティビティから大きな利益を得るプロセスです。

もちろん、セキュリティのためのHI分割製造設計は、単なるインターフェイスピンの難読化ではありません。まず、そのようなシステムに対するセキュリティ攻撃の現在および将来のモデルの両方を理解する必要があります。これらの攻撃は動的で予測が困難ですが、既存の攻撃と潜在的な脆弱性を明確に理解すると、システムセキュリティの全体的な設計に大きく役立ちます。また、攻撃者がこれらの攻撃面のプロパティをリバースエンジニアリングすることの難しさを評価するために、意味のあるメトリックを開発する必要があります。分割製造コンセプトは、さまざまなサプライヤーのチップの内部機能の主要な制御された変更を推進して、難読化を最大化することもできます。FPGAなどの動的に構成可能なコンポーネントの組み込みも検討する必要があります。このHIスペースにEDAツールベンダーが関与すると、ピン割り当てだけでなく、ルーティング、チップ機能、さらにはシステムアーキテクチャにおいても、非常に曖昧で安全な変更が行われる可能性があります。システムのコスト、面積、消費電力の関数としてのシステムセキュリティの改善を評価する必要があります。

D. EMサイドチャネル攻撃（SCA）耐性のシミュレーション

EM SCAの改善されたシミュレーションは、結合効果のモデリング、トランジスタレベルでの過渡信号の分析、マッチング回路、およびEMフィールドの計算を必要とする既存のEM SCAシミュレーションに関連するコストと複雑さを軽減するために提案されています。提案されたEMのシミュレーションフローは、EMトレースの高速かつ正確な予測を可能にし、SCAに対するこれらのシステムの復元力を可能にするため、重要です。コストの削減は、a）意図しない情報が漏洩する可能性のある重要な時期にのみトランジスタレベルのシミュレーションを実行するための商用CADツールを使用して実現されます。およびb）EM放射が上部メタライゼーション層の電源/グラウンド相互接続の電流に制限されるという事実。EMのシミュレーションでは、異なる暗号化ブロックのEMトレースを並列で実行する必要もあります。これにより、シミュレーション時間が大幅に短縮されます。

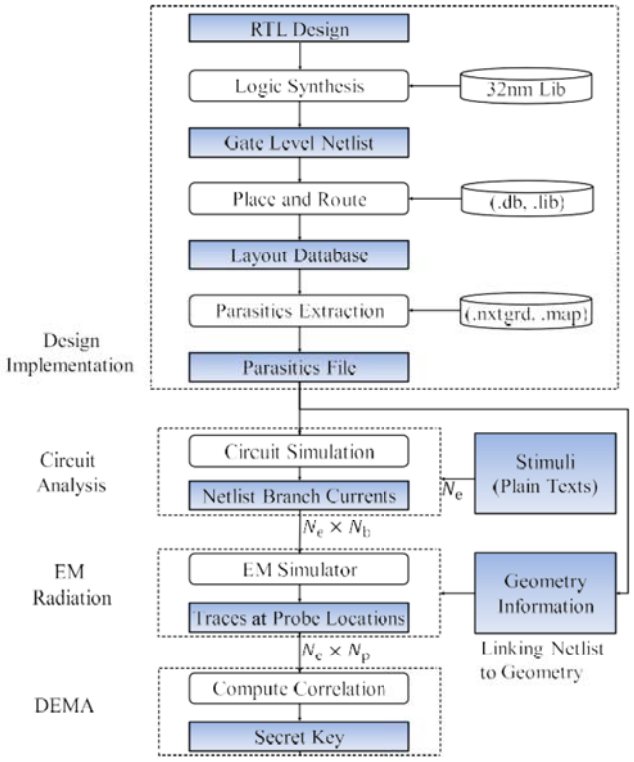


Figure 8: EM side-channel attack vulnerability analysis.[13]

提案された設計フローとSCA脆弱性の評価手順を図8に示します。これは、IC設計のRTL記述から始まります。ただし、差別化されたEM攻撃（DEMA）は信号をリークする暗号実行フェーズに焦点を当てているため、すべての手順が実行されるわけではありません。AESの場合、これは最終ラウンドで発生することが示されています。EM信号の計算も、最上位のメタライゼーション層の電流のみを考慮することで削減されます。

提案されたフロー分析は並列実行を可能にするため、HIシステムでは特に魅力的です。たとえば、EMのシミュレーションは、攻撃者が観察できる暗号化スキームを実装しているHIシステムのすべての要素に対して並列に実行できます。このアプローチは、HIの各要素の脆弱性を特定し、HIのセキュリティを向上させるために何ができるかについての洞察を提供できます。たとえば、EMのシミュレーションを使用すると、プローブの場所に基づいて脆弱性のポイントを特定できます。VDD / VSSラインを不均一に配置することにより、セキュリティを解除するために必要なトレースの数は、これらのラインの均一な配置に対して最大5倍まで増加します。[13]

EMシミュレーションは、システムの脆弱性を低コストで高速に洞察できるため、重要です。これにより、EM SCAを困難にするICレイアウト設計の変更を評価できます。現在のアプローチは、HIシステムに必要な、伝送線路ベースのEMシミュレータと全波EMシミュレータに限定されています。これは、ヘテロジニアスシステムのさまざまな要素間の通信の脆弱性を予測する必要があるため、複雑なヘテロジニアスシステムにとっても重要です。

一般的に、タイミング、電力、EMなどのSCAからの保護には、いくつかのレベルでの対策の実装が必要になります[15]:リークを削減するためのトランジスタレベル、ランダム化操作のためのプログラムレベル、漏洩を減らす目的と、攻撃者が特定のキーを使用して提供できる計算を制限するプロトコルレベル。一般的なSCA保護には、設計者およびインテグレーターによるあらゆるレベルのセキュリティ問題の関与と理解が必要です。

セクション 4. 一般的な結論

明らかに、サイバーセキュリティはすべての電子システムにとって重要な関心事です。電子システムの複雑性と相互接続性の増加の一般的な傾向により、サイバーセキュリティは、特に生命にかかわる危険にさらされるアプリケーションの研究にとって、最優先事項の1つとなっています。この章では、より広範なサプライチェーン、より複雑なシステムトポロジ、及びヘテロジニアスインテグレーションによって駆動されるチップの近接性の増加によって最も影響を受けるサイバーセキュリティの脅威に対処しました。上記で詳細に説明したように、ヘテロジニアスインテグレーションは、相互接続レイアウト、テストプロトコル、サプライチェーンの多様化、及び垂直に積み重ねられた形状の変更により、セキュリティに大きな影響を与えます。これらの増加したセキュリティの脅威は、セキュリティに対する体系的な設計の観点を必要とするセキュリティへのよりシステムレベルのアプローチで対処する必要があることは明らかです。

攻撃用の多くの高帯域幅インターフェイスを備えた多様なサプライヤーのコモディティチップにセキュリティ用のパッチを追加しようとするだけで、新しい攻撃ベクトルが発見されるまで、セキュリティリスクはせいぜい遅れるだけです。本当に必要なのは、高度な認証、階層型セキュリティ、分割製造コンセプト、SCA緩和戦略などのイノベーションを使用して境界条件を根本的に変更する、システムレベルでのセキュリティ設計アプローチです。パッケージレベルでのHIのこのセキュリティ設計目標を達成するには、システムセキュリティをパフォーマンス、電力、面積などの他のメトリックとトレードオフするオプションとともに、パッケージレベルでのEDAツールの進歩が必要です。パッケージレベルの設計ツールには最近の進歩がありますが、これらにはセキュリティ中心のテストとメトリックを追加する必要があります。

適切な対策を講じないと、多くの異なるベンダーの近くにある多くのチップのHIが、これらのコンパクトなIoTシステムのサイバー攻撃に対する脆弱性の増加につながることを強調することが重要です。コスト、面積、消費電力、パフォーマンスへの悪影響を最小限に抑えながら、HI製品のセキュリティ強化を提供できるのは、基本的な理解、サプライヤー間の緊密な連携、セキュリティのための積極的なシステム設計を通じてのみです。

参考文献

[1] Extracted from “Research Needs for Secure, Trustworthy, and Reliable Semiconductors”, SRC workshop publication, 2013. https://www.src.org/library/publication/p066751/p066751.pdf#search=research%20needs%20for%20secure%20trustworthy

[2] Sohrab Aftabjahani and Steve Brown, “Taxonomy of Physical Attacks,” TrustHub, VulnerabilityDB, 2018. [Online]. Available http://www.trust-hub.org/vulnerabilityDB.php.

[3] Texas Instrument Literature Number: SNOA287. [Online]. Available http://www.ti.com/lit/an/snoa287/snoa287.pdf.

[4] R. Radojcic, More-than-Moore 2.5D and 3D Sip Integration, Springer, 2017.

[5] C.S. Kim, K.H. Jong, and S.J. Im, “Document watermarking based on digital holographic principle”, Institute of Optics, Department of Physics, Kim II Sung University, Pyongyan, DPR of Korea.

[6] E. Wang and Y. Zhao, “Etching of nanostructures on soda-lime glass”, Optics Letters, Vol 39, 2014, p. 3748-3751.

[7] R. Elnaggar and M. Tahoori, “Run-Time Hardware Trojan Detection Using Performance Counters”, Proceedings of the International Test Conference, 2017.

[8] E. J. Marinissen, T. McLaurin and Hailong Jiao, "IEEE Std P1838: DfT standard-under-development for 2.5D-, 3D-, and 5.5D-SICs," 2016 21th IEEE European Test Symposium (ETS), Amsterdam, 2016, pp. 1-10.

[9] J. Dworak, Z. Conroy, A. Crouch and J. Potter, "Board security enhancement using new locking SIB-based architectures," 2014 International Test Conference, Seattle, WA, 2014, pp. 1-10.

[10] X. Wang, Y. Zheng, A. Basak and S. Bhunia, "IIPS: Infrastructure IP for Secure SoC Design," in IEEE Transactions on Computers, vol. 64, no. 8, pp. 2226-2238, Aug. 1 2015.

[11] A. Basak, S. Bhunia, T. Tkacik and S. Ray, "Security Assurance for System-on-Chip Designs With Untrusted IPs," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1515-1528, July 2017.

[12] J. Dofe, Q. Yu, H. Zhang, and E. Salman, Proc. Great Lakes Symposium on VLSI (GLSVLSI16), pp. 96-74, May 2016.

[13] A. Kumar, C. Scarborough, A. Yilmaz and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, 2017, pp. 123-130.

[14] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis”, Advances in Cryptology, pp. 789, Springer Berlin/Heidelberg, 1999.

[15] G. Bertoni, J. Daemen, M. Peeters and G. Van Assche, “Note on side-channel attacks and their countermeasures”, [Online]. Available at https://keccak.team

Edited by Paul Wesling