ハードウェアセキュリティ

永田　真（神戸大学）
nagata@cs.kobe-u.ac.jp

1. ハードウェアセキュリティとは

ディジタル情報の流通と利活用は社会活動の基盤であり，データの機密性，完全性，可用性を確保するセキュリティの必然性は自明であろう．ハードウェアセキュリティは，ディジタル情報を扱う情報デバイスに関するセキュリティ技術の全体を包含する概念である[1]．情報デバイスは，データの入手，記憶，処理，出力を担い，その機能，性能，仕様，信頼性，セキュリティ等の技術要件を満たすように設計・製造される．更に，ハードウェアセキュリティの視点からは，機能の停止，劣化あるいは改ざん等の意図しない変更が生じていないことについて検証される必要がある．このような変更は，悪意ある第三者による行為，若しくは経年や周囲環境との相互作用等の自然発生的な経過により引き起こされる可能性がある．

ハードウェアセキュリティのカバーする技術範囲は広く，情報デバイスの多様な構成原理と要求機能にまたがって議論される．図1に示すように，代表的な研究領域である①暗号技術の実装と運用，②半導体チップの真正性，③計測セキュリティが密接に相互関連し，サイバーフィジカルシステムやデータ駆動形システムにおけるセキュリティを実現している．一般に，情報デバイスの主な構成要素は半導体集積回路（IC：Integrated Circuit）であることから，ハードウェアセキュリティと半導体技術は密接に関連している．

2. 暗号技術の実装と運用

データの守秘や真正を保証するために暗号技術が利用される．暗号アルゴリズムは共通鍵方式と公開鍵方式に大別され，いずれも計算機上のソフトウェアモジュールあるいは半導体チップ上のICモジュールとしてユーザが利用可能な形式に具現される（この過程を実装とも呼称する）．

共通鍵方式の暗号アルゴリズムは，データの転置や置換等のビットレベル処理に基づいて構成されることが多く，小形，省電力かつ高速な実装が探求されている．共通鍵暗号の国際的な標準規格であるAdvanced Encryption Standard（AES）や軽量暗号と分類される暗号アルゴリズムが知られており，情報処理デバイスにおける暗号技術としてあまねく利用されている．

公開鍵方式の暗号アルゴリズムは，データを離散対数問題の特性を応用して（暗号化と復号に対して非対象に）数式処理する．多ビットの算術演算（加算，減算，乗算，除算）を繰り返すため，大規模な演算器を必要とし，長大なクロックサイクル数を消費する傾向にある．近年，データを暗号化したまま計算する（あるいは検索する）機能，ユーザの属性により復号の可否を制御する機能，あるいは量子コンピュータの登場により懸念される暗号の解読性を回避する耐量子性の獲得など，高機能暗号への展開が活発に探求されている．このような背景から，公開鍵方式の暗号アルゴリズムを高性能に実装するプログラミング技術や集積回路技術の開発は盛んである[2]．

一般に，国際的に標準化された暗号アルゴリズムは，暗号工学や暗号理論に基づいて堅ろうであること，すなわち，第三者による暗号文の解読が通常のコストでは不可能であるこ

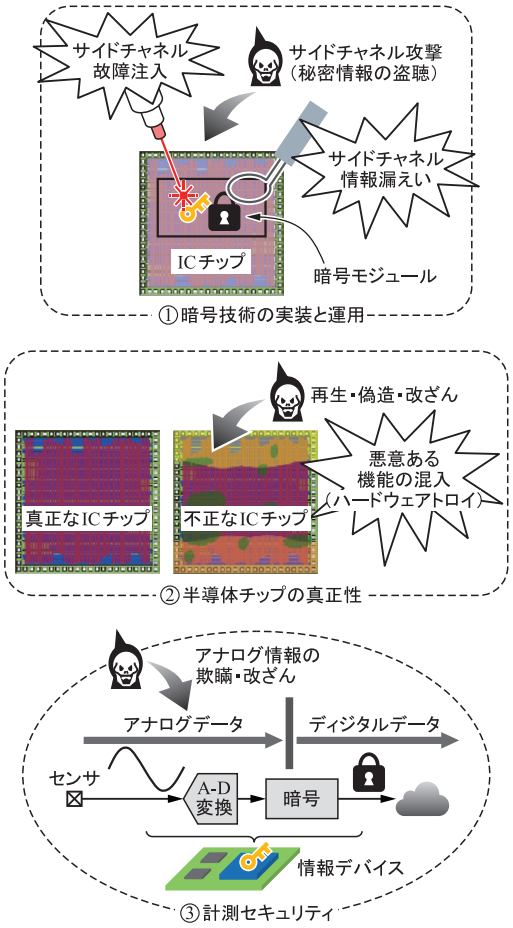

図1　ハードウェアセキュリティ　　情報デバイスの実装におけるセキュリティ技術の全体を包含する幅広い研究領域である．

本会ハンドブック「知識の森」
https://www.ieice-hbkb.org/portal/doc_index.html

とについて数理的に証明されている．その一方で，暗号アルゴリズムが暗号モジュールに実装されると，暗号化・復号における入力データと出力データの関係（正規のデータチャネル）には現れないぜい弱性が発現することが知られている．例えば，暗号化・復号の過程で消費される電力やクロックサイクル数，あるいは暗号モジュールから放射される電磁波等の物理情報には，暗号アルゴリズムにおけるデータ処理との相関が隠されている．更に，暗号モジュールの動作中にビットレベルの故障を注入する（ビットレベルのデータ変更を引き起こす）ことで意図的に誘発する暗号文の誤りにも同種の相関が隠されている．このような傍流の情報（サイドチャネル情報）を大量に収集し，暗号モジュールの論理動作を考慮した統計処理を施すことで，暗号モジュールの内部で秘匿されている秘密鍵のデータを推定できる可能性があり，サイドチャネル情報漏えいと呼ばれる．悪意ある第三者がサイドチャネル情報漏えいを利用して秘密情報を盗聴することを，サイドチャネル攻撃と呼び，暗号モジュールを危たい化する脅威として具体的に報告されている．暗号モジュールの設計者は，サイドチャネル攻撃による秘密情報の推定可能性を探索し，対策する．サイドチャネル攻撃耐性の獲得は，暗号アルゴリズムを具現する物理層の広大な技術領域（アーキテクチャ，回路，パッケージング，材料など）において横断的に候補技術が見いだされており，ハードウェアセキュリティにおける主要な研究課題の一つである．

3. 半導体チップの真正性

半導体チップの設計・製造・流通・廃棄のライフサイクルは，世界規模の多国籍企業やサプライチェーンの下で展開され，年間一兆個を超える半導体チップが国際的に調達されている．半導体チップは，前述の暗号モジュールやトレーサビリティに向けた自己識別機能を搭載し，現代社会におけるセキュリティ基盤として，例えば社会経済活動の基盤となる重要インフラ等[3]のディジタル化を支える情報デバイスの基幹部品として位置付けられている．このような背景の下，近年，半導体チップの真正性，すなわち，半導体チップが正規の設計・製造者から正しい流通経路の下で入手されたものであるか，について検証する技術と枠組みの構築が世界的に進められている．

半導体チップのライフサイクルに関与するステークホルダーの裾野は広く，真正性を危たい化する可能性の排除には多大な努力が求められる．半導体チップの再生，模造あるいは改ざんなど，不正な半導体チップの問題は，半導体市場の形成とともに顕在化してきた．不正な半導体チップが流通する市場について統計情報が報告され，また，半導体業界による警鐘も示されている[4]．昨今，経済安全保障における重要課題の一つとして，米国・欧州・アジアの政策的な取組みも目立っている[5]．

先進国で廃棄された情報デバイスから半導体チップが取り外され，新品同様に再生されて市場に投入される．あるいは，半導体チップから設計情報を抽出して模造する，更には，特定の動作条件において情報漏えいを引き起こす特殊機能（ハードウェアトロイ）を付与して製造する，など悪性の高いシナリオが考えられる．最先端の情報デバイスの開発・製造は深い階層構造を有するため，下流の工程において不正な半導体チップがサブシステムに混入してしまうと，より上流の工程では正規品として扱われてしまう．このような情報デバイスが正規品として市場に投入されると，その購入者は，信頼性の著しく劣化した状態に陥る，あるいは不正な機能が発現する，など，思いがけずセキュリティ課題に直面することになる．

半導体チップの真正性を保証する，あるいは，不正品の混入を排除する手段として，IC 設計データに不正な機能が含まれないことを検証する技術，IC チップを搭載したプリント回路基板の改ざんを見抜く技術等の報告があり，ハードウェアセキュリティの研究領域として活発である．

4. 計測セキュリティ

サイバーフィジカルシステムにおいては，人々の生活する物理空間におけるアナログ情報を，ディジタルデータとして計算機環境（サイバー空間）に取り込み，ディジタルツインや機械学習など最新の情報工学に基づく情報処理を行い，その結果を物理世界にフィードバックする．近年，アナログ物理情報の検知（センシング）や作用（アクチュエーション）におけるセキュリティの課題が指摘され，その対策はますます重要になっている．例えば，自動運転による車両の運行において，周囲環境のセンシングや制動にかかるアクチュエーションに関するセキュリティの危たい化を避けなければならない．車両と障害物の距離を計測する手段として，光学カメラにより撮像した画像データの解析，あるいはミリ波レーダの照射に対する反射波の解析が知られるが，攻撃者による擬似画像の提示や擬似波の照射等による欺瞞の可能性は排除できず，実証実験やシミュレーションによる検証手法について学術的に報告されている．

アナログ物理情報の計測機能やアナログ―ディジタル変換機能（あるいはディジタル―アナログ変換機能）に関して，その動作原理に依拠したセキュリティ機構の開発が求められる．アナログ領域のセキュリティを，ディジタル領域のセキュリティ，すなわち暗号アルゴリズムの実装や運用と統合することで，物理空間とサイバー空間を横断する計測セキュリティ技術の構築につながる．ハードウェアセキュリティ分野の新しい研究領域として活発に探求されている．

文　　献

（1） 電子情報通信学会ハードウェアセキュリティ研究会，委員会概要（2023 年 8 月アクセス）．
https://www.ieice.org/ess/hws/hws

（2） T. Matsumoto, M. Ikeda, M. Nagata, and Y. Uemura, “Secure cryptographic unit as root-of-trust for IoT era,” IEICE Trans. Electron., vol. E104-C, no. 7, pp. 262-271, July 2021. DOI:10.1587/transele.2020CDI0001

（3） 内閣サイバーセキュリティセンター，重要インフラとは（2023 年 8 月アクセス）．
https://www.nisc.go.jp/policy/group/infra/index.html

（4） 永田　真，“IC チップの真正性の確保と対策―ハードウェアセキュリティの根源的課題に向き合う―，”信学 FR 誌，vol. 8 no. 3, pp. 177-182, Jan. 2015. DOI:10.1587/ESSFR.8.177

（5） 永田　真，“IC チップのサプライチェーン・セキュリティ―真正性を脅かす課題と対策―，”信学 FR 誌，vol. 16, no. 2, pp. 93-99, Oct. 2022. DOI:10.1587/essfr.16.2_93

（2023 年 8 月 28 日受付）