2021 年 7 月 15 日

ニュースリリース

量子トンネル半導体 IP は、既知のあらゆる IoT 攻撃から安全であることが確認

量子駆動型デバイスフィンガープリントが、独立系検証機関が試みたすべてのサイドチャネル攻撃を防御

IoT 向け量子駆動型サイバー・セキュリティ・スペシャリストの英 Crypto Quantique は、独立検証の結果、第 2 世代の物理複製困難関数（PUF）向けの同社 CMOS 半導体 IP を使用して、CMOS チップ用の不変かつ偽造不能である一意のフィンガープリントを作成しても、サイドチャネル攻撃が防御されることを発表しました。これは、独立系のサイバーセキュリティ検証機関である eShard 社が、3 か月にわたって調査した結果、明らかになったものです。eShard 社で CEO を務める Hugues Thiebeauld 氏は、次のように述べています。「当社のセキュリティアナリストが Crypto Quantique のテストチップにおける近接場電磁放射を精査した結果、QDID アナログ IP に関して、当該製品が EAL4+認定（注）に必要な優れた防御力を備えていると結論付けました」

Crypto Quantique の PUF である QDID は、微小な量子トンネル電流を測定できるため、サイドチャネル攻撃に弱い他のチップセキュリティ技術に比べて高い堅牢性を備えています。サイドチャネル攻撃は、暗号鍵による変量を特定することでビット値を抽出します。たとえば、あるセルが 0 状態よりも 1 状態のときに電力消費量が多い場合、その差異を測定することで、半導体内に秘匿されている ID と暗号鍵が暴露される可能性があります。この問題を軽減する技術は存在しますが、高額であるため導入は容易ではありません。これを解決するのが QDID です。QDID により、半導体メーカーはシンプルかつ低コストで、IoT デバイスの厳しいセキュリティ要件に対応できるようになります。高額な対策を導入しなくても、デバイスについて EAL4+のセキュリティを確保することが可能です。

QDID フィンガープリントは、デバイスの ID と暗号鍵をオンデマンドで生成するための乱数またはシードで、この ID と暗号鍵を合わせて使用することで、チップまたはデバイスのためのハードウェア Root of Trust（RoT）が形成され、それが IoT デバイスのセキュリティの基礎になります。

QDID IP では、2 個のトランジスターで構成されたセルによる 64 x 64 のセルアレイが形成されます。この技術では、CMOS 酸化物層を通る量子トンネルを利用します。この層を通じて、特定の部位の厚みと原子構造に応じた深度まで電子が伝搬されます。この場合の物理的特性の相違は完全にランダムであり、製造段階で調整することはできません。この場合の電流は、フェムトアンペア（10^{-15} アンペア）または数十単位の電子の精度で決定されます。QDID はこの電子流を正確に測定し、隣接するセルの数値に基づいて 1s または 0s をランダムに生成します。

Crypto Quantique で CEO を務める Shahram Mossayebi は、次のように述べています。「デバイス ID と暗号鍵に対するサイドチャネル攻撃は、IoT エッジデバイスのセキュリティに対する最大の脅威となっています。独立機関による今回の評価を通じて、IoT デバイスの中核にある半導体は、量子駆動のエントロピーを利用して安全な ID と暗号鍵を生成することで、EAL4+のセキュリティを簡単かつ低コストで確保できることが示されました。この場合、乱数がすべてオンデマンドで生成され、保存の必要がないため、鍵の導入によって発生し得るセキュリティ上の大きな弱点が解消されます」

注: 評価保証レベル（EAL）は、コモンクライテリア（CC）に基づくセキュリティ評価の結果に応じて、製品またはシステムに付与される等級です。

###

Crypto Quantique について

英国ロンドンに本社を置く Crypto Quantique は、暗号システムのエキスパートである Shahram Mossayebi 博士（CEO）と、複雑な並列コンピューターシステムに関する豊富な経験を持つ半導体設計者の Patrick Camilleri 博士（CTO）が共同で設立した企業です。同社は、世界最高のセキュアなエンドツーエンドの IoT セキュリティ・プラットフォームを開発していますが、その核心にあるのが、世界初の量子力学に基づく半導体ハードウェア IP の QDID です。QDID により、標準の CMOS プロセスによって製造されたデバイス向けに、偽造不可能な一意の暗号鍵が複数生成されます。この暗号鍵は保存する必要がなく、独立して複数の用途にオンデマンドで使用できます。Crypto Quantique の汎用型 IoT セキュリティ・プラットフォーム、QuarkLink の暗号化 API と組み合わせれば、シリコン、デバイス、ソフトウェア、ソリューションプロバイダー間を安全につなぐことが可能です。企業詳細はこちらをご参照ください（www.cryptoquantique.com）。
Crypto Quantique の LinkedIn、 Twitter

eShard について

eShard は、フランスのボルドーに本社を置き、マルセイユとシンガポールの支社を加えて 30 人に及ぶ専門家を擁し、チップ製造と組み込みソフトウェアのセキュリティ分野で優れた技術を提供しています。同社は 2015 年以来、欧州、北米、アジアに事業を展開し、STMicroelectronics、Thales、V-Key Visa を始めとする、40 社にのぼる大手企業にサービスを提供しています。防衛、航空宇宙、金融、ハイテク、保健衛生、半導体の各分野で、最先端のソフトウェアスイートにより、サイバーセキュリティ（データ、トランザクション、知的財産の保護）に関する複雑な課題の解決を支援しています。このターンキーソリューションは、チップ、組み込みソフトウェア、モバイルアプリケーションの侵入防御をライフサイクル全体にわたってテストします。企業詳細はこちらをご参照ください（www.eshard.com）をご参照ください。
eShard の LinkedIn、Twitter

メディアのお問い合わせ先

Bob Jones、Crypto Quantique
bjones@cryptoquantique.com
ミアキス・アソシエイツ　本田
honda@miacis.jp